Moscow Journal of Combinatorics and Number Theory

2019
vol. 8 no. 2

On the quotient set of the distance set

Alex Iosevich, Doowon Koh and Hans Parshall

msp

Moscow Journal of Combinatorics and Number Theory
Vol. 8, No. 2, 2019
dx.doi.org/10.2140/moscow.2019.8.103

On the quotient set of the distance set

Alex Iosevich, Doowon Koh and Hans Parshall

Let $\mathbb{F}_q$ be a finite field of order q. We prove that if $d \geq 2$ is even and $E \subset \mathbb{F}_q^d$ with $|E| \geq 9q^{d/2}$ then

$$\mathbb{F}_q = \frac{\Delta(E)}{\Delta(E)} = \left\{ \frac{a}{b} : a \in \Delta(E), b \in \Delta(E) \backslash \{0\} \right\},$$

where

$$\Delta(E) = \{\|x-y\| : x, y \in E\}, \quad \|x\| = x_1^2 + x_2^2 + \cdots + x_d^2.$$

If the dimension d is odd and $E \subset \mathbb{F}_q^d$ with $|E| \geq 6q^{d/2}$, then

$$\{0\} \cup \mathbb{F}_q^+ \subset \frac{\Delta(E)}{\Delta(E)},$$

where $\mathbb{F}_q^+$ denotes the set of nonzero quadratic residues in $\mathbb{F}_q$. Both results are, in general, best possible, including the conclusion about the nonzero quadratic residues in odd dimensions.

1. Introduction

The Erdős–Falconer distance problem in vector spaces over finite fields asks for the smallest possible size of

$$\Delta(E) = \{\|x-y\| : x, y \in E\}, \quad \|x\| = x_1^2 + \cdots + x_d^2,$$

given $E \subset \mathbb{F}_q^d$, $d \geq 2$. This problem was introduced by Bourgain, Katz and Tao [Bourgain et al. 2004]. Here $\mathbb{F}_q$ denotes the finite field with q elements and $\mathbb{F}_q^d$ is the d-dimensional vector space over this field.

In [Iosevich and Rudnev 2007], one of us and Misha Rudnev proved that if $E \subset \mathbb{F}_q^d$, $d \geq 2$, with $|E| > 2q^{(d+1)/2}$, then $\Delta(E) = \mathbb{F}_q$. Hart, Rudnev and two of us [Hart et al. 2011] showed that, in a sense, this result is best possible when d is odd. More precisely, for any $c \in (0, 1)$ and any q sufficiently large with respect to c, they construct subsets $E \subset \mathbb{F}_q^d$ with $|E| > \frac{c}{2}q^{(d+1)/2}$ but $|\Delta(E)| < cq$. This construction does not appear to generalize to the even-dimensional case. In [Chapman et al. 2012], Chapman, Erdoğan, Hart and two of us proved that if q is prime, $q \equiv 3 \pmod 4$ and if $E \subset \mathbb{F}_q^2$ with $|E| \geq Cq^{4/3}$ for a sufficiently large constant $C > 0$, then

$$|\Delta(E)| > \frac{q}{2}.$$

This result was extended to two-dimensional vector spaces over arbitrary finite fields in [Bennett et al. 2017]. In even dimensions $d \geq 2$, it is reasonable to conjecture that if $|E| \geq Cq^{d/2}$ with a sufficiently large C, then $|\Delta(E)| > \frac{1}{2}q$, but this conjecture currently remains open. The exponent $\frac{d}{2}$ cannot be

MSC2010: 11T24, 52C17.
Keywords: quotient set, distance set, finite field.

improved. To see this, let $q = p^2$, p prime, and let $E = \mathbb{F}_p^d \subset \mathbb{F}_q^d$. Then $|E| = q^{d/2}$, yet $\Delta(E) = \mathbb{F}_p$. When q is a prime and $d \geq 4$, the sharpness of $\frac{d}{2}$ can be demonstrated using Lagrangian subspaces [Hart et al. 2011]. In two dimensions, the sharpness of $\frac{d}{2} = 1$ is easily demonstrated by taking a suitable subset of a straight line.

The purpose of this paper is to show that under the assumption $|E| \geq Cq^{d/2}$, taking the quotient of the elements of $\Delta(E)$ recovers all of $\mathbb{F}_q$ for d even, and at least all the square elements of $\mathbb{F}_q$ when d is odd. More precisely, for $E \subset \mathbb{F}_q^d$ we define

$$\frac{\Delta(E)}{\Delta(E)} := \left\{ \frac{a}{b} : a \in \Delta(E),\ b \in \Delta(E) \backslash \{0\} \right\}.$$

Our main results are the following.

Theorem 1.1. *Let $E \subset \mathbb{F}_q^d$, d even. Then if $|E| \geq 9q^{d/2}$, we have*

$$\mathbb{F}_q = \frac{\Delta(E)}{\Delta(E)}.$$

Theorem 1.2. *Let $d \geq 3$ be an odd integer and $E \subset \mathbb{F}_q^d$. Then if $|E| \geq 6q^{d/2}$, we have*

$$\{0\} \cup \mathbb{F}_q^+ \subset \frac{\Delta(E)}{\Delta(E)}.$$

Sharpness of results. The results are in general sharp up to constants. To see this, we once again take $q = p^2$ and $E = \mathbb{F}_p^2$. Then $|E| = q^{d/2}$; yet

$$\left\{ \frac{a}{b} : a \in \Delta(E),\ b \in \Delta(E) \backslash \{0\} \right\} = \mathbb{F}_p.$$

The statement about the squares in Theorem 1.2 is also sharp. The example in [Hart et al. 2011, page 15] that illustrates the sharpness of the exponent $(d+1)/2$ yields a set of size $cq^{(d+1)/2}$, with c sufficiently small, such that $\Delta(E) \subset \{(a-a')^2 : a, a' \in A\}$, where A is a suitable arithmetic progression in $\mathbb{F}_q$. In particular, $\Delta(E)$ is a subset of the squares, so the ratios of the elements of $\Delta(E)$ are also squares.

2. Proof of Theorem 1.1

For $t \in \mathbb{F}_q$, let

$$\nu(t) = \sum_{x,y \in \mathbb{F}_q^d} E(x)E(y)S_t(x-y),$$

where

$$S_t = \{x \in \mathbb{F}_q^d : \|x\| = t\}.$$

It is clear that $0 \in \Delta(E)/\Delta(E)$ unless $\Delta(E) = \{0\}$. Thus it suffices to prove that for each $r \neq 0$ there exists $t \in \Delta(E) \setminus \{0\}$ such that $tr \in \Delta(E)$. Since $t \in \Delta(E)$ if and only if $\nu(t) > 0$, we must show that for any $r \in \mathbb{F}_q^*$,

$$\nu^2(0) < \sum_{t \in \mathbb{F}_q} \nu(t)\nu(rt). \tag{2-1}$$

We shall need the following standard Fourier-analytic preliminaries. Given $f : \mathbb{F}_q^d \to \mathbb{C}$, define the Fourier transform $\hat{f}$ by the formula

$$\hat{f}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(-x \cdot m) f(x),$$

where χ is a nontrivial principal character on $\mathbb{F}_q$. We shall use the following calculation repeatedly.

Lemma 2.1. *With the notation above,*

$$f(x) = \sum_{m \in \mathbb{F}_q^d} \chi(x \cdot m) \hat{f}(m) \qquad \text{(Fourier inversion)}$$

and

$$\sum_{m \in \mathbb{F}_q^d} |\hat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{F}_q^d} |f(x)|^2. \qquad \text{(Plancherel)}$$

By Fourier inversion,

$$\nu(t) = q^{2d} \sum_{m \in \mathbb{F}_q^d} \widehat{S}_t(m) |\widehat{E}(m)|^2 = q^{-d} |E|^2 |S_t| + q^{2d} \sum_{m \neq \vec{0}} \widehat{S}_t(m) |\widehat{E}(m)|^2.$$

It follows that for $r \in \mathbb{F}_q^*$,

$$\begin{aligned}
\sum_{t \in \mathbb{F}_q} \nu(t)\nu(rt) &= \sum_{t \in \mathbb{F}_q} \Big(q^{-d} |E|^2 |S_t| + q^{2d} \sum_{m \neq \vec{0}} \widehat{S}_t(m) |\widehat{E}(m)|^2 \Big) \Big(q^{-d} |E|^2 |S_{rt}| + q^{2d} \sum_{m' \neq \vec{0}} \widehat{S}_{rt}(m') |\widehat{E}(m')|^2 \Big) \\
&= q^{-2d} |E|^4 \sum_{t \in \mathbb{F}_q} |S_t| |S_{rt}| + q^d |E|^2 \sum_{m' \neq \vec{0}} |\widehat{E}(m')|^2 \sum_{t \in \mathbb{F}_q} |S_t| \widehat{S}_{rt}(m') \\
&\quad + q^d |E|^2 \sum_{m \neq \vec{0}} |\widehat{E}(m)|^2 \sum_{t \in \mathbb{F}_q} |S_{rt}| \widehat{S}_t(m) + q^{4d} \sum_{m, m' \neq \vec{0}} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2 \sum_{t \in \mathbb{F}_q} \widehat{S}_t(m) \widehat{S}_{rt}(m') \\
&= I + II + III + IV.
\end{aligned} \tag{2-2}$$

We shall invoke the explicit value of $|S_t|$, which can be deduced by Theorem 6.26 in [Lidl and Niederreiter 1997].

Lemma 2.2. *Let $S_t \subset \mathbb{F}_q^d$ denote the sphere with radius $t \in \mathbb{F}_q$. Then if $d \geq 2$ is even,*

$$|S_t| = q^{d-1} + \lambda(t) q^{(d-2)/2} \eta((-1)^{d/2}),$$

where η is the quadratic character of $\mathbb{F}_q^*$, $\lambda(t) = -1$ for $t \in \mathbb{F}_q^*$, and $\lambda(0) = q - 1$.

We also use the following result, which was given as Lemma 4 in [Iosevich and Koh 2010].

Lemma 2.3. *Let S_j be a sphere in $\mathbb{F}_q^d$, $d \geq 2$. Then for any $m \in \mathbb{F}_q^d$, we have*

$$\widehat{S}_j(m) = q^{-1} \delta_0(m) + q^{-d-1} \eta^d(-1) G^d \sum_{s \in \mathbb{F}_q^*} \eta^d(s) \chi\left(js + \frac{\|m\|}{4s} \right),$$

where G denotes the Gauss sum, η is the quadratic character of $\mathbb{F}_q^*$, and $\delta_0(m) = 1$ if $m = (0, \ldots, 0)$ and $\delta_0(m) = 0$ otherwise.

A lower bound of $\sum_{t\in\mathbb{F}_q} \nu(t)\nu(rt)$ for even dimensions $d \geq 2$. Since $\sum_{t\in\mathbb{F}_q}\lambda(rt)=0$ for $r\neq 0$, it follows from Lemma 2.2 that

$$\begin{aligned} I &:= q^{-2d}|E|^4\sum_{t\in\mathbb{F}_q}|S_t||S_{rt}| = q^{-2d}|E|^4\Big(q^{2d-1}+q^{d-2}\sum_{t\in\mathbb{F}_q}\lambda(t)\lambda(rt)\Big)\\ &= q^{-2d}|E|^4\Big(q^{2d-1}+q^{d-2}\lambda^2(0)+q^{d-2}\sum_{t\neq 0}\lambda(t)\lambda(rt)\Big)\\ &= q^{-2d}|E|^4\big(q^{2d-1}+q^{d-2}(q-1)^2+q^{d-2}(q-1)\big).\end{aligned}$$

Hence, we obtain

$$I = q^{-1}|E|^4+q^{-d}|E|^4-q^{-d-1}|E|^4. \tag{2-3}$$

In order to estimate the remaining terms, we need the following calculations.

Lemma 2.4. *Suppose that $m\neq\vec{0}$ in $\mathbb{F}_q^d$, $d\geq 2$. Then for any $r\neq 0$, we have*

$$\sum_{t\in\mathbb{F}_q}\widehat{S}_{rt}(m)=0, \tag{2-4}$$

$$\sum_{t\in\mathbb{F}_q}\lambda(t)\widehat{S}_{rt}(m)=q\widehat{S}_0(m), \tag{2-5}$$

where $\lambda(t)$ is defined as in Lemma 2.2.

To see this, observe that the left-hand side of (2-4) equals

$$q^{-d}\sum_{t\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q^d}\chi(-x\cdot m)S_{rt}(x) = q^{-d}\sum_{x\in\mathbb{F}_q^d}\chi(-x\cdot m)\sum_{t\in\mathbb{F}_q}S_{rt}(x) = q^{-d}\sum_{x\in\mathbb{F}_q^d}\chi(-x\cdot m)=0$$

since $m\neq(0,\ldots,0)$. Hence (2-4) follows. By the definition of $\lambda(t)$,

$$\sum_{t\in\mathbb{F}_q}\lambda(t)\widehat{S}_{rt}(m)=(q-1)\widehat{S}_0(m)-\sum_{t\neq 0}\widehat{S}_{rt}(m)=(q-1)\widehat{S}_0(m)-\sum_{t\in\mathbb{F}_q}\widehat{S}_{rt}(m)+\widehat{S}_0(m).$$

Then (2-5) follows by (2-4). This completes the proof of Lemma 2.4.

We shall also need the following orthogonality lemma.

Lemma 2.5. *Suppose that $r\in\mathbb{F}_q^*$ and $m, m'\in\mathbb{F}_q^d$. If $d\geq 2$ is even, then we have*

$$\sum_{t\in\mathbb{F}_q}\widehat{S}_t(m)\widehat{S}_{rt}(m') = \begin{cases} q^{-1}\delta_0(m)\delta_0(m')+q^{-d}-q^{-d-1} & \text{if } \|m\|=r\|m'\|,\\ -q^{-d-1} & \text{if } \|m\|\neq r\|m'\|.\end{cases}$$

The proof shall be given at the end of the paper (see Lemma 4.2). With the lemmas in tow, we are ready to handle terms II, III and IV. In view of Lemmas 2.2 and 2.4, if $m'\neq\vec{0}$, then

$$\sum_{t\in\mathbb{F}_q}|S_t|\widehat{S}_{rt}(m') = q^{d-1}\sum_{t\in\mathbb{F}_q}\widehat{S}_{rt}(m')+q^{(d-2)/2}\eta((-1)^{d/2})\sum_{t\in\mathbb{F}_q}\lambda(t)\widehat{S}_{rt}(m') = q^{d/2}\eta((-1)^{d/2})\widehat{S}_0(m').$$

Using this equation, it follows that

$$II := q^d|E|^2 \sum_{m'\neq\vec{0}} |\widehat{E}(m')|^2 \sum_{t\in\mathbb{F}_q} |S_t|\widehat{S}_{rt}(m') = q^{3d/2}\eta((-1)^{d/2})|E|^2 \sum_{m'\neq\vec{0}} |\widehat{E}(m')|^2\widehat{S}_0(m').$$

By the same argument, it is not difficult to see that $II = III$. Namely, we have

$$II + III = 2q^{3d/2}\eta((-1)^{d/2})|E|^2 \sum_{m\neq\vec{0}} |\widehat{E}(m)|^2\widehat{S}_0(m). \tag{2-6}$$

We now move on to the term

$$IV := q^{4d} \sum_{m,m'\neq\vec{0}} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2 \sum_{t\in\mathbb{F}_q} \widehat{S}_t(m)\widehat{S}_{rt}(m').$$

Using Lemma 2.5, we can write $IV = A + B$, where

$$A = -q^{3d-1} \sum_{\substack{\|m\|\neq r\|m'\| \\ m,m'\neq\vec{0}}} |\widehat{E}(m)|^2|\widehat{E}(m')|^2,$$

$$B = (q^{3d} - q^{3d-1}) \sum_{\substack{\|m\|=r\|m'\| \\ m,m'\neq\vec{0}}} |\widehat{E}(m)|^2|\widehat{E}(m')|^2.$$

It follows that

$$IV = A + B = q^{3d} \sum_{\substack{\|m\|=r\|m'\| \\ m,m'\neq\vec{0}}} |\widehat{E}(m)|^2|\widehat{E}(m')|^2 - q^{3d-1} \sum_{m,m'\neq\vec{0}} |\widehat{E}(m)|^2|\widehat{E}(m')|^2 = A' - B'.$$

Combining this with (2-3), (2-6), we obtain that if $d \geq 2$ is even and $r \neq 0$, then

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} \nu(t)\nu(rt) &= I + II + III + IV \\ &= (q^{-1}|E|^4 + q^{-d}|E|^4 - q^{-d-1}|E|^4) \\ &\qquad + 2q^{3d/2}\eta((-1)^{d/2})|E|^2\Big(\sum_{m\neq\vec{0}} |\widehat{E}(m)|^2\widehat{S}_0(m)\Big) + (A' - B').\end{aligned}$$

Notice that each term above is a real number. It follows that

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} \nu(t)\nu(rt) &\geq q^{-1}|E|^4 - 2q^{3d/2}|E|^2\big(\max_{m\neq\vec{0}} |\widehat{S}_0(m)|\big)\Big(\sum_{m\in\mathbb{F}_q^d} |\widehat{E}(m)|^2\Big) + (A' - B') \\ &= q^{-1}|E|^4 - 2q^{d/2}|E|^3\big(\max_{m\neq\vec{0}} |\widehat{S}_0(m)|\big) + (A' - B'),\end{aligned}$$

where we used the Plancherel theorem, which states

$$\sum_{m\in\mathbb{F}_q^d} |\widehat{E}(m)|^2 = q^{-d}|E|.$$

By the definitions of A' and B', we see that

$$A'-B' \ge q^{3d}\Big(\sum_{\substack{\|m\|=0\\ m\neq\vec{0}}} |\widehat{E}(m)|^2\Big)^2 - q^{3d-1}\Big(\sum_{m\in\mathbb{F}_q^d} |\widehat{E}(m)|^2\Big)^2 = q^{3d}\Big(\sum_{\substack{\|m\|=0\\ m\neq\vec{0}}} |\widehat{E}(m)|^2\Big)^2 - q^{d-1}|E|^2.$$

We also see from Lemma 2.3 that if $d \ge 2$ is even, then

$$\max_{m\neq\vec{0}} |\widehat{S}_0(m)| \le q^{-d/2}.$$

Thus we conclude that if $d \ge 2$ is even and $r \neq 0$, then

$$\sum_{t\in\mathbb{F}_q} \nu(t)\nu(rt) \ge q^{-1}|E|^4 - 2|E|^3 + q^{3d}\Big(\sum_{\substack{\|m\|=0\\ m\neq\vec{0}}} |\widehat{E}(m)|^2\Big)^2 - q^{d-1}|E|^2. \tag{2-7}$$

An upper bound of $\nu^2(0)$ for even dimensions $d \ge 2$. It follows that

$$\nu(0) = q^{2d}\sum_{m\in\mathbb{F}_q^d} \widehat{S}_0(m)|\widehat{E}(m)|^2.$$

By Lemma 2.3, notice that if $d \ge 2$ is even, then

$$\widehat{S}_0(m) = q^{-1}\delta_0(m) + q^{-d-1}G^d \sum_{s\in\mathbb{F}_q^*} \chi(s\|m\|).$$

Then we see that

$$\nu(0) = q^{-1}|E|^2 + q^{d-1}G^d \sum_{m\in\mathbb{F}_q^d} |\widehat{E}(m)|^2\Big(-1 + \sum_{s\in\mathbb{F}_q} \chi(s\|m\|)\Big).$$

By the Plancherel theorem and the orthogonality of χ,

$$\nu(0) = q^{-1}|E|^2 - q^{-1}G^d|E| + q^d G^d \sum_{\|m\|=0} |\widehat{E}(m)|^2.$$

Since $\widehat{E}(\vec{0}) = q^{-d}|E|$, we can write

$$\nu(0) = q^{-1}|E|^2 - q^{-1}G^d|E| + q^{-d}G^d|E|^2 + q^d G^d \sum_{\substack{\|m\|=0\\ m\neq\vec{0}}} |\widehat{E}(m)|^2. \tag{2-8}$$

We shall use the following explicit form of the Gauss sum G.

Lemma 2.6 [Lidl and Niederreiter 1997, Theorem 5.15]. *Let $\mathbb{F}_q$ be a finite field with $q = p^\ell$ for an odd prime p and $\ell \in \mathbb{N}$. Then the Gauss sum G satisfies*

$$G = \begin{cases} (-1)^{\ell-1}q^{1/2} & \text{if } p \equiv 1 \pmod 4,\\ (-1)^{\ell-1}i^\ell q^{1/2} & \text{if } p \equiv 3 \pmod 4.\end{cases}$$

Observe from Lemma 2.6 that if the dimension d is even, then $G^d = \pm q^{d/2}$, where the sign depends on d and q. Combining this observation with (2-8), and considering the sign of each term, we see that if d is even, then

$$\nu(0) \le \begin{cases} q^{-1}|E|^2 + q^{(d-2)/2}|E| & \text{if } G^d = -q^{d/2}, \\ q^{-1}|E|^2 + q^{-d/2}|E|^2 + q^{3d/2}\sum_{\|m\|=0, m\ne\vec{0}} |\widehat{E}(m)|^2 & \text{if } G^d = q^{d/2}. \end{cases}$$

Assuming that $|E| \ge q^{d/2}$, we see that

$$\nu(0) \le \begin{cases} 2q^{-1}|E|^2 & \text{if } G^d = -q^{d/2}, \\ 2q^{-1}|E|^2 + q^{3d/2}\sum_{\|m\|=0, m\ne\vec{0}} |\widehat{E}(m)|^2 & \text{if } G^d = q^{d/2}. \end{cases}$$

Since $\nu(0)$ is a nonnegative real number, it follows that if $|E| \ge q^{d/2}$, then

$$\nu^2(0) \le 4q^{-2}|E|^4 + 4q^{(3d-2)/2}|E|^2 \sum_{\substack{\|m\|=0 \\ m\ne\vec{0}}} |\widehat{E}(m)|^2 + q^{3d}\Bigg(\sum_{\substack{\|m\|=0 \\ m\ne\vec{0}}} |\widehat{E}(m)|^2\Bigg)^2.$$

Since

$$\sum_{\substack{\|m\|=0 \\ m\ne\vec{0}}} |\widehat{E}(m)|^2 \le \sum_{m\in\mathbb{F}_q^d} |\widehat{E}(m)|^2 = q^{-d}|E|,$$

we conclude that if $|E| \ge q^{d/2}$, then

$$\nu^2(0) \le 4q^{-2}|E|^4 + 4q^{(d-2)/2}|E|^3 + q^{3d}\Bigg(\sum_{\substack{\|m\|=0 \\ m\ne\vec{0}}} |\widehat{E}(m)|^2\Bigg)^2. \tag{2-9}$$

Now we are ready to complete the proof of Theorem 1.1.

Complete proof of Theorem 1.1. We must show that (2-1) holds. By (2-7) and (2-9), it is enough to show that if $|E| \ge 9q^{d/2}$, then

$$q^{-1}|E|^4 - 2|E|^3 - q^{d-1}|E|^2 > 4q^{-2}|E|^4 + 4q^{(d-2)/2}|E|^3.$$

It suffices to show that

$$q^{-1}|E|^4 - 6q^{(d-2)/2}|E|^3 - q^{d-1}|E|^2 > 4q^{-2}|E|^4.$$

If $|E| \ge 9q^{d/2}$, then we see that

$$q^{-1}|E|^4 - 6q^{(d-2)/2}|E|^3 - q^{d-1}|E|^2 \ge \tfrac{1}{3}q^{-1}|E|^4 - q^{d-1}|E|^2,$$

so it is sufficient to show that

$$\tfrac{1}{3}q^{-1}|E|^4 - q^{d-1}|E|^2 > 4q^{-2}|E|^4.$$

Observe that if $|E| \ge 9q^{d/2} (\ge \sqrt{12}q^{d/2})$, then

$$\tfrac{1}{3}q^{-1}|E|^4 - q^{d-1}|E|^2 \ge \tfrac{1}{4}q^{-1}|E|^4.$$

Consequently, it suffices to show that

$$\tfrac{1}{4}q^{-1}|E|^4 > 4q^{-2}|E|^4,$$

which holds if $q > 16$. Therefore, when $q \le 16$, it suffices to prove the statement of Theorem 1.1. More precisely, it remains to show that if $|E| \ge 9q^{d/2}$ and $q \le 16$, then $\mathbb{F}_q = \Delta(E)/\Delta(E)$. Since $9q^{d/2} > 2q^{(d+1)/2}$ for $q \le 16$, it will be enough to prove that if $|E| > 2q^{(d+1)/2}$, then $\Delta(E) = \mathbb{F}_q$. This was proved in [Iosevich and Rudnev 2007]. Thus the proof of Theorem 1.1 is complete.

3. Proof of Theorem 1.2

We proceed as in the proof of Theorem 1.1. As seen in (2-2), for $r \in \mathbb{F}_q^+$, we can write

$$\begin{aligned}\sum_{t\in\mathbb{F}_q} \nu(t)\nu(rt) &= \sum_{t\in\mathbb{F}_q}\Big(q^{-d}|E|^2|S_t| + q^{2d}\sum_{m\neq\vec{0}}\widehat{S}_t(m)|\widehat{E}(m)|^2\Big)\Big(q^{-d}|E|^2|S_{rt}| + q^{2d}\sum_{m'\neq\vec{0}}\widehat{S}_{rt}(m')|\widehat{E}(m')|^2\Big)\\
&= q^{-2d}|E|^4\sum_{t\in\mathbb{F}_q}|S_t||S_{rt}| + q^d|E|^2\sum_{m'\neq\vec{0}}|\widehat{E}(m')|^2\sum_{t\in\mathbb{F}_q}|S_t|\widehat{S}_{rt}(m')\\
&\quad + q^d|E|^2\sum_{m\neq\vec{0}}|\widehat{E}(m)|^2\sum_{t\in\mathbb{F}_q}|S_{rt}|\widehat{S}_t(m) + q^{4d}\sum_{m,m'\neq\vec{0}}|\widehat{E}(m)|^2|\widehat{E}(m')|^2\sum_{t\in\mathbb{F}_q}\widehat{S}_t(m)\widehat{S}_{rt}(m')\\
&= \mathrm{I}+\mathrm{II}+\mathrm{III}+\mathrm{IV}.\end{aligned}$$

The following explicit value of $|S_t|$ is given as Theorem 6.27 in [Lidl and Niederreiter 1997].

Lemma 3.1. *Let $S_t \subset \mathbb{F}_q^d$ denote the sphere with radius $t \in \mathbb{F}_q$. If $d \ge 3$ is odd, then*

$$|S_t| = q^{d-1} + q^{(d-1)/2}\eta((-1)^{(d-1)/2}t),$$

where η denotes the quadratic character of $\mathbb{F}_q^*$ and $\eta(0) = 0$.

We recall from Lemma 2.3 that if $d \ge 3$ is odd, then for any $m \in \mathbb{F}_q^d$,

$$\widehat{S}_j(m) = q^{-1}\delta_0(m) + q^{-d-1}\eta(-1)G^d\sum_{s\in\mathbb{F}_q^*}\eta(s)\chi\Big(js + \frac{\|m\|}{4s}\Big). \tag{3-1}$$

Estimate of $\sum_{t\in\mathbb{F}_q}\nu(t)\nu(rt)$ for odd dimensions $d \ge 3$. Since $\sum_{t\in\mathbb{F}_q^*}\eta(t) = 0$ (by the orthogonality of η) and $\eta(0) = 0$, it follows from Lemma 3.1 that

$$\begin{aligned}\mathrm{I} &:= q^{-2d}|E|^4\sum_{t\in\mathbb{F}_q}|S_t||S_{rt}|\\
&= q^{-2d}|E|^4\sum_{t\in\mathbb{F}_q}\big(q^{d-1}+q^{(d-1)/2}\eta((-1)^{(d-1)/2}t)\big)\big(q^{d-1}+q^{(d-1)/2}\eta((-1)^{(d-1)/2}rt)\big)\\
&= q^{-2d}|E|^4\Big(\sum_{t\in\mathbb{F}_q}q^{2d-2} + \sum_{t\in\mathbb{F}_q}q^{d-1}\eta(r)\eta^2(t)\Big) = q^{-2d}|E|^4\big(q^{2d-1}+q^{d-1}\eta(r)(q-1)\big).\end{aligned}$$

Since $\eta(r) = 1$ (by the assumption that $r \in \mathbb{F}_q^+$), we have

$$\mathrm{I} \ge q^{-1}|E|^4.$$

In order to estimate the second term II, we begin by proving the following result.

Lemma 3.2. *Let S_j be the sphere in $\mathbb{F}_q^d$ for odd $d \geq 3$. Then for $r \neq 0$ and $m \neq \vec{0}$, we have*

$$\Omega := \sum_{t\in\mathbb{F}_q} |S_t|\widehat{S}_{rt}(m) = q^{(-d-3)/2} G^{d+1} \eta(r\,(-1)^{(d+1)/2}) \Big(-1 + \sum_{s\in\mathbb{F}_q} \chi(s\|m\|)\Big).$$

To prove this lemma, recall from (2-4) of Lemma 2.4 that $\sum_{t\in\mathbb{F}_q} \widehat{S}_{rt}(m) = 0$ for $r \neq 0$ and $m \neq \vec{0}$. By Lemma 3.1,

$$\Omega = \sum_{t\in\mathbb{F}_q} \big(q^{d-1} + q^{(d-1)/2}\eta((-1)^{(d-1)/2}t)\big)\widehat{S}_{rt}(m) = q^{(d-1)/2}\eta((-1)^{(d-1)/2}) \sum_{t\in\mathbb{F}_q} \eta(t)\widehat{S}_{rt}(m).$$

By using the value of $\widehat{S}_{rt}(m)$ in (3-1), we can write

$$\Omega = q^{(-d-3)/2}\eta((-1)^{(d+1)/2})G^d \sum_{s\neq 0} \eta(s)\chi\Big(\frac{\|m\|}{4s}\Big)\Big(\sum_{t\in\mathbb{F}_q} \eta(t)\chi(rst)\Big).$$

Since $\eta(0) = 0$ and $\eta(a) = \eta(a^{-1})$ for $a \neq 0$, a simple change of variables yields

$$\sum_{t\in\mathbb{F}_q} \eta(t)\chi(rst) = \eta(rs)G$$

and thus we have

$$\Omega = q^{(-d-3)/2}\eta((-1)^{(d+1)/2})G^{d+1}\eta(r) \sum_{s\neq 0} \chi(s\|m\|),$$

which completes the proof of Lemma 3.2.

By Lemma 3.2 and the orthogonality of χ, we see that

$$\begin{aligned}
\mathrm{II} &:= q^d|E|^2 \sum_{m'\neq\vec{0}} |\widehat{E}(m')|^2 \sum_{t\in\mathbb{F}_q} |S_t|\widehat{S}_{rt}(m') \\
&= q^{(d-1)/2}|E|^2G^{d+1}\eta(r\,(-1)^{(d+1)/2}) \sum_{\substack{m'\neq\vec{0}\\ \|m'\|=0}} |\widehat{E}(m')|^2 - q^{(d-3)/2}|E|^2G^{d+1}\eta(r\,(-1)^{(d+1)/2}) \sum_{m'\neq\vec{0}} |\widehat{E}(m')|^2 \\
&= \mathrm{II}_1 - \mathrm{II}_2.
\end{aligned}$$

Now observe from Lemma 2.6 that $G^{d+1} \in \mathbb{R}$ for odd d and so both II_1 and II_2 are real numbers. Furthermore, both values are real numbers with the same sign. Hence, $\mathrm{II} = \mathrm{II}_1 - \mathrm{II}_2 \geq \min\{-|\mathrm{II}_1|, -|\mathrm{II}_2|\}$. Since

$$\min\{-|\mathrm{II}_1|, -|\mathrm{II}_2|\} \geq -\big|q^{(d-1)/2}|E|^2G^{d+1}\eta(r\,(-1)^{(d+1)/2})\big| \sum_{m'\in\mathbb{F}_q^d} |\widehat{E}(m')|^2,$$

which is same as $-|E|^3$, we obtain that

$$\mathrm{II} \geq -|E|^3.$$

By the same argument, it is not hard to see that $\mathrm{II} = \mathrm{III}$ and we also have

$$\mathrm{III} \geq -|E|^3.$$

In order to estimate the fourth term IV, we shall need the following orthogonality lemma.

Lemma 3.3. *Suppose that $r \in \mathbb{F}_q^*$ and $m, m' \in \mathbb{F}_q^d$. If $d \geq 3$ is odd, then we have*

$$\sum_{t \in \mathbb{F}_q} \widehat{S}_t(m) \widehat{S}_{rt}(m') = \begin{cases} q^{-1}\delta_0(m)\delta_0(m') + (q^{-d} - q^{-d-1})\eta(r) & \text{if } \|m\| = r\|m'\|, \\ -q^{-d-1}\eta(r) & \text{if } \|m\| \neq r\|m'\|, \end{cases}$$

where η denotes the quadratic character of $\mathbb{F}_q^*$.

The proof shall be given at the end of the paper (see Lemma 4.2). By the definition of the term IV and Lemma 3.3, it follows that

$$\begin{aligned} \mathrm{IV} &:= q^{4d} \sum_{m, m' \neq \vec{0}} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2 \sum_{t \in \mathbb{F}_q} \widehat{S}_t(m) \widehat{S}_{rt}(m') \\ &= -q^{3d-1}\eta(r) \sum_{\substack{m, m' \neq \vec{0} \\ \|m\| \neq r\|m'\|}} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2 + (q^{3d} - q^{3d-1})\eta(r) \sum_{\substack{m, m' \neq \vec{0} \\ \|m\| = r\|m'\|}} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2. \end{aligned}$$

Since $\eta(r) = 1$ (by our assumption that r is a square number in $\mathbb{F}_q^*$), the second term above is positive. Thus we have

$$\mathrm{IV} \geq -q^{3d-1} \sum_{m, m' \in \mathbb{F}_q^d} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2.$$

By the Plancherel theorem,

$$\mathrm{IV} \geq -q^{d-1}|E|^2.$$

Putting this together with all other estimates, we obtain that if $d \geq 3$ is odd and r is a square number, then

$$\sum_{t \in \mathbb{F}_q} \nu(t)\nu(rt) := \mathrm{I} + \mathrm{II} + \mathrm{III} + \mathrm{IV} \geq q^{-1}|E|^4 - 2|E|^3 - q^{d-1}|E|^2. \tag{3-2}$$

Estimate of $\nu^2(0)$ for odd dimensions $d \geq 3$. Recall that we can write

$$\nu(0) = q^{2d} \sum_{m \in \mathbb{F}_q^d} \widehat{S}_0(m) |\widehat{E}(m)|^2 = q^{2d} \widehat{S}_0(\vec{0}) |\widehat{E}(\vec{0})|^2 + q^{2d} \sum_{m \neq \vec{0}} \widehat{S}_0(m) |\widehat{E}(m)|^2 := M + R.$$

Since $|S_0| = q^{d-1}$ for odd $d \geq 3$ (see Lemma 3.1),

$$M = q^{-d}|S_0|\,|E|^2 = q^{-1}|E|^2.$$

To estimate R, observe that

$$R \leq q^{2d} \big(\max_{m \neq \vec{0}} |\widehat{S}_0(m)|\big) \bigg(\sum_{m \in \mathbb{F}_q^d} |\widehat{E}(m)|^2 \bigg) = \big(\max_{m \neq \vec{0}} |\widehat{S}_0(m)|\big) q^d |E|.$$

By (3-1), we see that if $d \geq 3$ is odd and $m \neq \vec{0}$, then

$$\widehat{S}_0(m) = q^{-d-1}\eta(-1) G^d \sum_{s \neq 0} \eta(s) \chi\left(\frac{\|m\|}{4s} \right).$$

Since

$$\left|\sum_{s\neq 0}\eta(s)\chi\left(\frac{\|m\|}{4s}\right)\right| = \sqrt{q}$$

for $\|m\| \neq 0$ and 0 otherwise, we see

$$\max_{m\neq\vec{0}} |\widehat{S}_0(m)| \leq q^{(-d-1)/2}.$$

Hence we obtain

$$R \leq q^{(d-1)/2}|E|.$$

We have seen that $\nu(0) := M + R \leq q^{-1}|E|^2 + q^{(d-1)/2}|E|$, which in turn implies

$$\nu^2(0) \leq q^{-2}|E|^4 + 2q^{(d-3)/2}|E|^3 + q^{d-1}|E|^2, \tag{3-3}$$

since $\nu(0)$ is a nonnegative integer.

Complete proof of Theorem 1.2. Let $d \geq 3$ be odd. Suppose that r is a square number in $\mathbb{F}_q^*$. We must show that if $E \subset \mathbb{F}_q^d$ with $|E| \geq 6q^{d/2}$, then

$$\sum_{t\in\mathbb{F}_q} \nu(t)\nu(rt) > \nu^2(0).$$

By (3-2) and (3-3), it will be enough to show that if $|E| \geq 6q^{d/2}$, then

$$q^{-1}|E|^4 - 2|E|^3 - q^{d-1}|E|^2 > q^{-2}|E|^4 + 2q^{(d-3)/2}|E|^3 + q^{d-1}|E|^2.$$

Note that to prove this it suffices to show that

$$q^{-1}|E|^4 - 4q^{(d-3)/2}|E|^3 - 2q^{d-1}|E|^2 > q^{-2}|E|^4.$$

If $|E| \geq 6q^{d/2} (\geq 6q^{(d-1)/2})$, then we see that

$$q^{-1}|E|^4 - 4q^{(d-3)/2}|E|^3 - 2q^{d-1}|E|^2 \geq \tfrac{1}{3}q^{-1}|E|^4 - 2q^{d-1}|E|^2.$$

Hence it is sufficient to show that if $|E| \geq 6q^{d/2}$, then

$$\tfrac{1}{3}q^{-1}|E|^4 - 2q^{d-1}|E|^2 > q^{-2}|E|^4.$$

Observe that if $|E| \geq 6q^{d/2} (\geq \sqrt{24}q^{d/2})$, then

$$\tfrac{1}{3}q^{-1}|E|^4 - 2q^{d-1}|E|^2 \geq \tfrac{1}{4}q^{-1}|E|^4.$$

In conclusion, it is enough to prove that if $|E| \geq 6q^{d/2}$, then

$$\tfrac{1}{4}q^{-1}|E|^4 > q^{-2}|E|^4,$$

which is clearly true provided that $q > 4$. For this reason, it suffices to prove the statement of Theorem 1.2 in the case when $q \leq 4$ and $|E| \geq 6q^{d/2}$. In other words, our task is to prove that if $|E| \geq 6q^{d/2}$ for $q \leq 4$, then $\mathbb{F}_q = \Delta(E)/\Delta(E)$. Since $6q^{d/2} > 2q^{(d+1)/2}$ for $q \leq 4$, it will be enough to show that if $|E| > 2q^{(d+1)/2}$, then $\Delta(E) = \mathbb{F}_q$. This is a well-known result on the Erdős–Falconer distance problem shown in [Iosevich and Rudnev 2007]. Thus we finish the proof of Theorem 1.2.

4. Proofs of Lemmas 2.5 and 3.3

We begin by proving the following lemma.

Lemma 4.1. *Let $r \in \mathbb{F}_q^*$ and $m, m' \in \mathbb{F}_q^d$. Then we have*

$$\sum_{t\in\mathbb{F}_q} \widehat{S}_t(m)\widehat{S}_{rt}(m') = \begin{cases} q^{-1}\delta_0(m)\delta_0(m') + q^{-2d}G^{2d}\eta^d(-r)(1-q^{-1}) & \text{if } \|m\| = r\|m'\|, \\ -q^{-2d-1}G^{2d}\eta^d(-r) & \text{if } \|m\| \neq r\|m'\|. \end{cases}$$

Proof. By Lemma 2.3, we have

$$\widehat{S}_t(m) = q^{-1}\delta_0(m) + q^{-d-1}\eta^d(-1)G^d \sum_{s\in\mathbb{F}_q^*} \eta^d(s)\chi\left(ts + \frac{\|m\|}{4s}\right) := A(t) + B(t),$$

$$\widehat{S}_{rt}(m') = q^{-1}\delta_0(m') + q^{-d-1}\eta^d(-1)G^d \sum_{s'\in\mathbb{F}_q^*} \eta^d(s')\chi\left(rts' + \frac{\|m'\|}{4s'}\right) := C(t) + D(t).$$

Since $\sum_{t\in\mathbb{F}_q} A(t)D(t) = 0 = \sum_{t\in\mathbb{F}_q} B(t)C(t)$ by the orthogonality of χ, we have

$$\begin{aligned}
\sum_{t\in\mathbb{F}_q} \widehat{S}_t(m)\widehat{S}_{rt}(m') &= \sum_{t\in\mathbb{F}_q} A(t)C(t) + \sum_{t\in\mathbb{F}_q} B(t)D(t) \\
&= q^{-1}\delta_0(m)\delta_0(m') + q^{-2d-2}G^{2d} \sum_{s,s'\in\mathbb{F}_q^*} \eta^d(s)\eta^d(s')\chi\left(\frac{\|m\|}{4s} + \frac{\|m'\|}{4s'}\right) \sum_{t\in\mathbb{F}_q} \chi(t(s+rs')) \\
&= q^{-1}\delta_0(m)\delta_0(m') + q^{-2d-1}G^{2d} \sum_{s\in\mathbb{F}_q^*} \eta^d(-s^2/r)\chi\left(\frac{\|m\|}{4s} - \frac{r\|m'\|}{4s}\right) \\
&= q^{-1}\delta_0(m)\delta_0(m') + q^{-2d-1}G^{2d}\eta^d(-r) \sum_{s\in\mathbb{F}_q^*} \chi(s(\|m\| - r\|m'\|)) \\
&= q^{-1}\delta_0(m)\delta_0(m') + \left[q^{-2d-1}G^{2d}\eta^d(-r) \sum_{s\in\mathbb{F}_q} \chi(s(\|m\| - r\|m'\|))\right] - q^{-2d-1}G^{2d}\eta^d(-r).
\end{aligned}$$

Thus the statement follows by the orthogonality of χ. $\square$

As a corollary of Lemma 4.1, one can deduce Lemmas 2.5 and 3.3 which can be restated as follows.

Lemma 4.2. *Suppose that $r \in \mathbb{F}_q^*$ and $m, m' \in \mathbb{F}_q^d$. If $d \geq 2$ is even, then we have*

$$\sum_{t\in\mathbb{F}_q} \widehat{S}_t(m)\widehat{S}_{rt}(m') = \begin{cases} q^{-1}\delta_0(m)\delta_0(m') + q^{-d} - q^{-d-1} & \text{if } \|m\| = r\|m'\|, \\ -q^{-d-1} & \text{if } \|m\| \neq r\|m'\|. \end{cases}$$

On the other hand, if $d \geq 3$ is odd, then we have

$$\sum_{t\in\mathbb{F}_q} \widehat{S}_t(m)\widehat{S}_{rt}(m') = \begin{cases} q^{-1}\delta_0(m)\delta_0(m') + (q^{-d} - q^{-d-1})\eta(r) & \text{if } \|m\| = r\|m'\|, \\ -q^{-d-1}\eta(r) & \text{if } \|m\| \neq r\|m'\|. \end{cases}$$

Proof. Suppose that $d \geq 2$ is even. Then $\eta^d = 1$. By Lemma 2.6, we see that $G^{2d} = q^d$ for even $d \geq 2$. Thus the statement follows by Lemma 4.1.

Next, assume that $d \geq 3$ is odd. Then $\eta^d = \eta$. Hence, by Lemma 4.1 it suffices to show that $G^{2d}\eta(-1) = q^d$ for odd $d \geq 3$. This equality follows by combining Lemma 2.6 with the facts that $\eta(-1) = 1$ for $q \equiv 1 \pmod 4$, and $\eta(-1) = -1$ for $q \equiv 3 \pmod 4$. □

References

[Bennett et al. 2017] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, "Group actions and geometric combinatorics in $\mathbb{F}_q^d$", *Forum Math.* **29**:1 (2017), 91–110. MR Zbl

[Bourgain et al. 2004] J. Bourgain, N. Katz, and T. Tao, "A sum-product estimate in finite fields, and applications", *Geom. Funct. Anal.* **14**:1 (2004), 27–57. MR Zbl

[Chapman et al. 2012] J. Chapman, M. B. Erdoğan, D. Hart, A. Iosevich, and D. Koh, "Pinned distance sets, k-simplices, Wolff's exponent in finite fields and sum-product estimates", *Math. Z.* **271**:1-2 (2012), 63–93. MR Zbl

[Hart et al. 2011] D. Hart, A. Iosevich, D. Koh, and M. Rudnev, "Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős–Falconer distance conjecture", *Trans. Amer. Math. Soc.* **363**:6 (2011), 3255–3275. MR Zbl

[Iosevich and Koh 2010] A. Iosevich and D. Koh, "Extension theorems for spheres in the finite field setting", *Forum Math.* **22**:3 (2010), 457–483. MR Zbl

[Iosevich and Rudnev 2007] A. Iosevich and M. Rudnev, "Erdős distance problem in vector spaces over finite fields", *Trans. Amer. Math. Soc.* **359**:12 (2007), 6127–6142. MR Zbl

[Lidl and Niederreiter 1997] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed., Encyclopedia of Mathematics and its Applications **20**, Cambridge University Press, 1997. MR Zbl

Received 5 Mar 2018. Revised 24 Nov 2018.

ALEX IOSEVICH:
iosevich@math.rochester.edu
Department of Mathematics, University of Rochester, Rochester, NY, United States

DOOWON KOH:
koh131@chungbuk.ac.kr
Department of Mathematics, Chungbuk National University, Cheongju, South Korea

HANS PARSHALL:
parshall.6@osu.edu
Department of Mathematics, The Ohio State University, Columbus, OH, United States

Moscow Journal of Combinatorics and Number Theory

msp.org/moscow

See inside back cover or msp.org/moscow for submission instructions.

The subscription price for 2019 is US $310/year for the electronic version, and $365/year (+$20, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Moscow Journal of Combinatorics and Number Theory (ISSN 2640-7361 electronic, 2220-5438 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

MJCNT peer review and production are managed by EditFlow® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Moscow Journal of Combinatorics and Number Theory
vol. 8 no. 2 2019