TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 363, Number 6, June 2011, Pages 3255–3275
S 0002-9947(2010)05232-8
Article electronically published on December 29, 2010

AVERAGES OVER HYPERPLANES, SUM-PRODUCT THEORY IN VECTOR SPACES OVER FINITE FIELDS AND THE ERDŐS-FALCONER DISTANCE CONJECTURE

DERRICK HART, ALEX IOSEVICH, DOOWON KOH, AND MISHA RUDNEV

Abstract. We prove a pointwise and average bound for the number of incidences between points and hyperplanes in vector spaces over finite fields. While our estimates are, in general, sharp, we observe an improvement for product sets and sets contained in a sphere. We use these incidence bounds to obtain significant improvements on the arithmetic problem of covering $\mathbb{F}_q$, the finite field with q elements, by $A \cdot A + \cdots + A \cdot A$, where A is a subset $\mathbb{F}_q$ of sufficiently large size. We also use the incidence machinery and develop arithmetic constructions to study the Erdős-Falconer distance conjecture in vector spaces over finite fields. We prove that the natural analog of the Euclidean Erdős-Falconer distance conjecture does not hold in this setting. On the positive side, we obtain good exponents for the Erdős-Falconer distance problem for subsets of the unit sphere in $\mathbb{F}_q^d$ and discuss their sharpness. This results in a reasonably complete description of the Erdős-Falconer distance problem in higher-dimensional vector spaces over general finite fields.

Contents

Received by the editors May 28, 2008 and, in revised form, September 26, 2009.
2010 *Mathematics Subject Classification.* Primary 42B05, 11T23, 52C10.

1. Introduction

Let $\mathbb{F}_q$ denote a finite field with q elements, where q, a power of an odd prime, is viewed as an asymptotic parameter. In the special case when $q = p$ is a prime, we use the notation $\mathbb{Z}_p$. Let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$. How large does $A \subset \mathbb{F}_q$ need to be to make sure that

$$dA^2 = \underbrace{A^2 + \cdots + A^2}_{d \text{ times}} \supseteq \mathbb{F}_q^*?$$

Define

$$A^2 = A \cdot A = \{a \cdot a' : a, a' \in A\} \text{ and } A + A = \{a + a' : a, a' \in A\}.$$

It is known (see e.g. [9]) that if $d = 3$ and q is prime, this conclusion holds if the number of elements $|A| \geq Cq^{\frac{3}{4}}$, with a sufficiently large constant $C > 0$. It is reasonable to conjecture that if $|A| \geq C_\epsilon q^{\frac{1}{2}+\epsilon}$, then $2A^2 \supseteq \mathbb{F}_q^*$. This result cannot hold, especially in the setting of general finite fields if $|A| = \sqrt{q}$, because A may in fact be a subfield. See also [2], [4], [8], [7], [11], [14], [19], [20] and the references contained therein on recent progress related to this problem and its analogs. For example, Glibichuk, [8], proved that

$$8A \cdot B = \mathbb{Z}_p,$$

p prime, provided that $|A||B| > p$ and either $A = -A$ or $A \cap (-A) = \emptyset$. Glibichuk and Konyagin, [9], proved that if A is subgroup of $\mathbb{Z}_p^*$, and $|A| > p^\delta$, $\delta > 0$, then

$$NA = \mathbb{Z}_p$$

with

$$N \geq C4^{\frac{1}{\delta}}.$$

The above-mentioned results were achieved by methods of arithmetic combinatorics.

One of the goals of this paper is to use the geometry of the vector space $\mathbb{F}_q^d$, where q is not necessarily a prime number, to deduce a good lower bound on the size of A that guarantees that $dA^2 \supseteq \mathbb{F}_q^*$.

The second aim of this paper is directly related to the finite field version of the Erdős-Falconer distance problem. The Erdős distance conjecture says that if E is a finite subset of $\mathbb{R}^d$, $d \geq 2$, then $|\Delta(E)| \geq C_\epsilon |E|^{\frac{2}{d}-\epsilon}$, where $\Delta(E) = \{\|x - y\| : x, y \in E\}$ and $\|\cdot\|$ denotes the standard Euclidean metric. This problem is far from resolution in any dimension. See, for example, a monograph by Matousek ([16]) and the references contained therein to review the main milestones of the progress towards this conjecture.

The Falconer distance conjecture says that if $E \subset \mathbb{R}^d$, $d \geq 2$, has Hausdorff dimension greater than $\frac{d}{2}$, then $\Delta(E)$ has positive Lebesgue measure. See [5] for the latest progress and description of techniques. For the connections between the Erdős and Falconer distance problems, see, for example, [13].

In the finite field setting, the question turns out to have features of both the Erdős and Falconer distance problems. The first nontrivial result was obtained by Bourgain, Katz and Tao ([3]) using arithmetic-combinatorial methods and the connection of the geometric incidence problem of counting distances with sum-product estimates.

Theorem 1.1 ([3]). *Suppose $E \subset \mathbb{Z}_p^2$, where $p \equiv 3 \mod 4$ is a prime, and $|E| \leq p^{2-\epsilon}$. Then there exists $\delta = \delta(\epsilon)$ such that*

$$|\Delta(E)| \geq c|E|^{\frac{1}{2}+\delta}.$$

Here and throughout the paper, for $E \subseteq \mathbb{F}_q^d$,

$$\Delta(E) = \{\|x-y\| = (x_1-y_1)^2 + \cdots + (x_d-y_d)^2 : x, y \in E\}$$

denotes the distance set of E.

It is interesting to observe that while the quantity $\|\cdot\|$ is not a distance, in the traditional sense, it is still a natural object in that it is invariant under the action of orthogonal matrices.

We note that the conclusion of Theorem 1.1 with the exponent $\frac{1}{2}$ follows from the argument due to Erdős ([6]). The condition $|E| \lesssim q^{2-\epsilon}$ addresses the fact that if $E = \mathbb{Z}_p^2$, then $\Delta(E) = \mathbb{Z}_p$ and so $|\Delta(E)| = \sqrt{|E|}$ and no better. The condition $p \equiv 3 \mod 4$ addresses the fact that if conversely $p \equiv 1 \mod 4$, the field $\mathbb{F}_p$ contains an element i such that $i^2 = -1$. This would allow one to take

$$E = \{(t, it) : t \in \mathbb{Z}_p\} \tag{1.1}$$

and it is straightforward to check that while $|E| = p$, $|\Delta(E)| = 1$ as all the distances between the elements of the set are identically 0.

In view of the examples cited in the previous paragraph, Iosevich and Rudnev ([12]) formulated the Erdős-Falconer conjecture as follows.

Conjecture 1.2 ([12]). *Let $E \subset \mathbb{F}_q^d$ such that $|E| \geq C_\epsilon q^{\frac{d}{2}+\epsilon}$. Then there exists $c > 0$ such that*

$$|\Delta(E)| \geq cq.$$

A Fourier analytic approach to this problem, developed in [12], led to the following result.

Theorem 1.3 ([12]). *Suppose that $E \subset \mathbb{F}_q^d$ and $|E| \geq 4q^{\frac{d+1}{2}}$. Then $\Delta(E) = \mathbb{F}_q$.*

If $d = 2$, in particular, whenever $q \ll |E| \ll q^2$, the results of the paper provide a quantitatively explicit estimate. This enabled the first two authors and J. Solymosi to use its analog to obtain a nontrivial sum-product estimate ([11]). The basis for the latter results was Weil's bound ([21]) for Kloosterman sums,

$$\left| \sum_{t \neq 0} \chi(at + t^{-1}) \right| \leq 2\sqrt{q},$$

where χ further denotes a nontrivial additive character of $\mathbb{F}_q$.

Observe that in the formulation of Conjecture 1.2 one asks for the *positive proportion* of distances in $\mathbb{F}_q$, while Theorem 1.3 guarantees that *all* distances in $\mathbb{F}_q$ occur, being generated by E. The latter question is closely related to what in the discrete Euclidean setting is known as the Erdős *single distance* conjecture, which

says that a single distance in $\mathbb{R}^2$ cannot occur more than $cn^{1+\epsilon}$ times, where n is the cardinality of the underlying point set E. It is tempting to strengthen the claim of Conjecture 1.2 to cover all distances. However, we shall see below that even the weak form of this conjecture (1.2) is not true. This shows that Theorem 1.3 is essentially sharp. This underlines the difference between the finite field setting and the Euclidean setting where the Erdős-Falconer distance conjecture, while far from being proved, is still strongly believed.

We shall see, however, that the exponent predicted by Conjecture 1.2 does hold for subsets of the sphere in

$$S^{d-1} = S = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}$$

in even dimensions. While it is possible that in some cases this exponent may be further improved for this class of sets under some circumstances, we provide examples showing that if one is after all the distances, and not a positive proportion, then getting a better index is not in general possible. This is geometrically analogous to the general case, for since S^{d-1} is a $(d-1)$-dimensional variety in $\mathbb{F}_q^d$, it makes sense that the sharp index should be $\frac{(d-1)+1}{2} = \frac{d}{2}$. The motivation for studying the Erdős-Falconer distance problems for subsets of the sphere is not limited by the consideration that it provides a large set of sets for which Conjecture 1.2 holds. For example, Erdős's original argument shows that N points in $\mathbb{R}^2$ determine $\gtrsim N^{\frac{1}{2}}$ distances by proceeding as follows. Choose one of the points in the set and draw circles of every possible radius centered at this point such that each circle contains at least one other point of the set. Suppose that the number of such circles is t. If $t \geq N^{\frac{1}{2}}$, we are done. If not, there exists a circle containing $\geq N/t$ points and these points, by an elementary argument, determine $\geq N/(2t)$ distinct distances. Comparing t and $N/(2t)$ yields the conclusion. In higher dimensions we may proceed by induction with the induction hypothesis being the number of distances determined by points on a sphere. Thus one may view the distribution of distances determined by points on a sphere as a natural and integral component of the general Erdős distance problem.

We conclude our introduction by emphasizing that the proofs below show that the arithmetic structure of general fields allows for examples that may not have analogs in Euclidean space. A detailed comparative study between the Euclidean and finite field environments shall be conducted in a subsequent paper.

2. Statement of results

2.1. **Key incidence estimate.** Our main tool is the following incidence theorem. See [10] for an earlier version.

Theorem 2.1. *Let $E \subset \mathbb{F}_q^d$ and define the* incidence function

$$\nu(t) = \{(x, y) \in E \times E : x \cdot y = t\}. \tag{2.1}$$

Then

$$\sum_{t \in \mathbb{F}_q} \nu^2(t) \leq |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq (0,\ldots,0)} |E \cap l_k| \left|\widehat{E}(k)\right|^2 + (q-1) q^{-1} |E|^2 E(0, \ldots, 0), \tag{2.2}$$

where

$$l_k = \{tk : t \in \mathbb{F}_q^*\}. \tag{2.3}$$

Moreover,

$$\nu(t) = |E|^2 q^{-1} + R(t), \tag{2.4}$$

with

$$\begin{cases} |R(t)| & \leq & |E| q^{\frac{d-1}{2}}, \quad \textit{for } t \neq 0, \\ |R(0)| & \leq & |E| q^{\frac{d}{2}}. \end{cases} \tag{2.5}$$

Note that $E(x)$ denotes the characteristic function of E, so $E(0,\dots,0) = 1$ if the origin is in E and 0 otherwise. Also note that in many of the applications below it is legitimate to assume, without loss of generality, that E does not in fact contain the origin.

Remark 2.2. The proof of Theorem 2.1 is via Fourier analysis. It has been pointed out to the authors by Seva Lev that an alternate approach to (2.4) is via a graph-theoretic result due to Alon and Krivelevich. See [1] and the references contained therein. We also note that the relevant result of Alon and Krivelevich can be recovered from the estimate (2.5) above.

Remark 2.3. There are parallels here that are worth pointing out. In the study of the Euclidean Falconer conjecture, the L^2 norm of the distance measure is dominated by the Mattila integral, discovered by P. Mattila, ([17]):

$$\int_1^\infty \left(\int_{S^{d-1}} |\widehat{\mu}(t\omega)|^2 d\omega \right)^2 t^{d-1} dt,$$

where μ is a Borel measure on the set E whose distance set is being examined. It is reasonable to view the expression

$$\sum_{k \neq (0,\dots,0)} |E \cap l_k| |\widehat{E}(k)|^2$$

as the Mattila integral for the dot product problem, a direct analog of the Mattila integral for the distance set problem in Euclidean space.

By analogy with the distance set $\Delta(E)$, let us introduce the set of dot products

$$\Pi(E) = \{x \cdot y = x_1 y_1 + \cdots + x_d y_d : x, y \in E\}. \tag{2.6}$$

Corollary 2.4. *Let $E \subset \mathbb{F}_q^d$ such that $|E| > q^{\frac{d+1}{2}}$. Then*

$$\mathbb{F}_q^* \subseteq \Pi(E).$$

This result cannot in general be improved in the following sense:

(i) *Whenever $\mathbb{F}_q$ is a quadratic extension, for any $\epsilon > 0$ there exists $E \subset \mathbb{F}_q^d$ of size $\approx q^{\frac{d+1}{2} - \epsilon}$ such that $|\Pi(E)| = o(q)$. In particular, the set of dot products does not contain a positive proportion of the elements of $\mathbb{F}_q$.*

(ii) *For $d = 4m + 3$, $m \geq 0$, for any $q \gg 1$ and any $t \in \mathbb{F}_q^*$, there exists E of cardinality $\approx q^{\frac{d+1}{2}}$ such that $t \notin \Pi(E)$.*

Throughout the paper, $X \lesssim Y$ means that there exists $C > 0$ such that $X \leq CY$.

2.2. **Arithmetic results.**

Theorem 2.5. *Let $A \subset \mathbb{F}_q$, where $\mathbb{F}_q$ is an arbitrary finite field with q elements, such that $|A| > q^{\frac{1}{2}+\frac{1}{2d}}$. Then*

$$\mathbb{F}_q^* \subset dA^2. \tag{2.7}$$

Moreover, suppose that for some constant $C_1^{\frac{1}{d}}$,

$$|A| \geq C_1^{\frac{1}{d}} q^{\frac{1}{2}+\frac{1}{2(2d-1)}}.$$

Then

$$|dA^2| \geq q \cdot \frac{C_1^{2-\frac{1}{d}}}{C_1^{2-\frac{1}{d}}+1}. \tag{2.8}$$

It follows immediately from Theorem 2.5 that in the most interesting particular case $d = 2$,

$$\mathbb{F}_q^* \subset A^2 + A^2 \quad \text{if} \quad |A| > q^{\frac{3}{4}}$$

and

$$|A^2 + A^2| \geq q \cdot \frac{C_1^{\frac{3}{2}}}{C_1^{\frac{3}{2}}+1} \quad \text{if} \quad |A| \geq C_1^{\frac{1}{2}} q^{\frac{2}{3}}.$$

We would like to complement the general result in Theorem 2.5 with the following conditional statement.

Theorem 2.6. *Let $A \subset \mathbb{F}_q$, with $|A| \geq C_1^{\frac{1}{2}} q^{\frac{1}{2}}$, and suppose that*

$$|(A \times A) \cap t(A \times A)| \leq C_2 |A|^2 q^{-1}, \tag{2.9}$$

for all $t \in \mathbb{F}_q^* \setminus \{1\}$. Then

$$|2A^2| \geq q \cdot \frac{C_1}{2C_1 + C_2}.$$

2.3. **Distance set results.**

Theorem 2.7. *The Conjecture 1.2 is false. More precisely, there exist $c > 0$ and $E \subset \mathbb{F}_q^d$, where d is odd, such that*

$$|E| \geq c q^{\frac{d+1}{2}} \quad \text{and} \quad \Delta(E) \neq \mathbb{F}_q.$$

Theorem 2.8. *Let $E \subset \mathbb{F}_q^d$, $d \geq 3$, be a subset of the sphere $S = \{x \in \mathbb{F}_q^d : \|x\| = 1\}$.*

(i) *Suppose that $|E| \geq C q^{\frac{d}{2}}$ with a sufficiently large constant C. Then there exists $c > 0$ such that*

$$|\Delta(E)| \geq cq. \tag{2.10}$$

(ii) *If d is even, then under the same assumptions as above,*

$$\Delta(E) = \mathbb{F}_q. \tag{2.11}$$

(iii) *If d is even, there exists $c > 0$ and $E \subset S$ such that*

$$|E| \geq c q^{\frac{d}{2}} \quad \text{and} \quad \Delta(E) \neq \mathbb{F}_q. \tag{2.12}$$

(iv) *If d is odd and $|E| \geq C q^{\frac{d+1}{2}}$ with a sufficiently large constant $C > 0$, then*

$$\Delta(E) = \mathbb{F}_q. \tag{2.13}$$

(v) *If d is odd, there exists $c > 0$ and $E \subset S$ such that*

$$|E| \geq cq^{\frac{d+1}{2}} \quad \textit{and} \quad \Delta(E) \neq \mathbb{F}_q. \tag{2.14}$$

Remark 2.9. In summary, we always get a positive proportion of all the distances if $|E| \geq Cq^{\frac{d}{2}}$. If d is even, we get all the distances under the same assumption and the size condition on E cannot be relaxed. Similarly, if d is odd we know that we cannot in general get all the distances if $|E| \ll q^{\frac{d+1}{2}}$, but, as we note above, we get a positive proportion of the distances under the assumption that $|E| \geq Cq^{\frac{d}{2}}$, and it is not out of the question that one can go as low as $q^{\frac{d-1}{2}+\epsilon}$, asking for the positive proportion of distances.

We conclude this section by formulating a result which says that if a subset of the sphere is statistically evenly distributed, then the distance set is large under much milder assumptions than above.

Definition 2.10. Let $E \subset S = \{x \in \mathbb{F}_q^d : x_1^2 + \cdots + x_d^2 = 1\}$. Suppose that

$$|E \cap H| \leq C|E|q^{-1}$$

for every $(d-1)$-dimensional hyperplane H passing through the origin. Then we say that E is uniformly distributed on the sphere.

We note that since the density of E is $\frac{|E|}{q^d}$ and the density of a hyperplane H is $\frac{|H|}{q^d} = q^{-1}$, the expected number of points on $E \cap H$ is indeed $q^d \cdot \frac{|E|}{q^d} \cdot q^{-1} = \frac{|E|}{q}$. Thus the uniformity assumption says that the number of points of E on each hyperplane through the origin does not exceed the expected number by more than a constant.

Theorem 2.11. *Suppose that E is uniformly distributed on the sphere and that $|E| \geq Cq$. Then*

$$|\Delta(E)| \geq cq. \tag{2.15}$$

2.4. **Acknowledgements.** The authors wish to thank Luca Brandolini, Leoardo Colzani, Giaccomo Gigante, Nets Katz, Sergei Konyagin, Seva Lev, Igor Shparlinsky and Ignacio Uriarte-Tuero for many helpful remarks about the content of this paper.

3. Proof of geometric results: Theorem 2.1 and Corollary 2.4

3.1. **Proof of the L^2 estimate (2.2).** The Fourier transform of a complex-valued function f on $\mathbb{F}_q^d$ with respect to a nontrivial principal additive character χ on $\mathbb{F}_q$ is given by

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

and the Fourier inversion formula takes the form

$$f(x) = \sum_{k \in \mathbb{F}_q^d} \chi(x \cdot k) \widehat{f}(k).$$

We have

$$\begin{aligned} \nu(t) &= |\{(x,y) \in E^2 : x \cdot y = t\}| \\ &= \textstyle\sum_{x \cdot y = t} E(x)E(y). \end{aligned}$$

The Cauchy-Schwarz inequality applied to the sum in the variable x yields

(3.1)
$$\begin{aligned}\sum_t \nu^2(t) &\le |E| \cdot \sum_t \sum_{x\cdot y=t} \sum_{x\cdot y'=t} E(x)E(y)E(y') \\ &= |E| \sum_{(y'-y)\cdot x=0} E(y')E(y)E(x) \\ &= |E| q^{-1} \sum_{y',y,x} \sum_s \chi(s((y'-y)\cdot x))E(y')E(y)E(x) \\ &= |E|^4 q^{-1} + |E| q^{2d-1} \sum_x \sum_{s\neq 0} E(x) \left|\widehat{E}(sx)\right|^2 \\ &= |E|^4 q^{-1} + |E| q^{2d-1} \sum_x \sum_{s\neq 0} E(sx) \left|\widehat{E}(x)\right|^2 \\ &= |E|^4 q^{-1} + |E| q^{2d-1} \sum_{x\neq(0,\dots,0)} |E\cap l_x| \left|\widehat{E}(x)\right|^2 + (q-1)q^{-1}|E|^3 E(0,\dots,0).\end{aligned}$$

In the third line we have used the standard trick that $\sum_{s\in\mathbb{F}_q} \chi(ts)$ equals q for $t=0$ and zero otherwise. The transition from the fourth line to the fifth one was after changing variables $sx \to x$ and then $s \to s^{-1}$. This completes the proof of the estimate (2.2), which uses the "Fourier" notation k for x.

3.2. **Proof of the pointwise estimate (2.4).** Similarly to the third line of (3.1), we rewrite the expression for the incidence function (2.1) in the form

$$\nu(t) = \sum_{x,y\in E} q^{-1} \sum_{s\in\mathbb{F}_q} \chi(s(x\cdot y - t)).$$

Isolating the term $s=0$ we have, according to (2.4),

(3.2)
$$\begin{aligned}\nu(t) &= |E|^2 q^{-1} + R(t), \quad \text{where} \\ R(t) &= \textstyle\sum_{x,y\in E} q^{-1} \sum_{s\neq 0} \chi(s(x\cdot y - t)).\end{aligned}$$

Viewing R as a sum in x, applying the Cauchy-Schwarz inequality and dominating the sum over $x\in E$ by the sum over $x\in\mathbb{F}_q^d$, we see that

$$\begin{aligned}R^2(t) &\le |E| \textstyle\sum_{x\in\mathbb{F}_q^d} q^{-2} \sum_{s,s'\neq 0} \sum_{y,y'\in E} \chi(sx\cdot y - s'x\cdot y')\chi(t(s'-s)) \\ &= |E| q^{d-2} \textstyle\sum_{\substack{sy=s'y' \\ s,s'\neq 0}} \chi(t(s'-s))E(y)E(y') \\ &= I + II,\end{aligned}$$

where the term I corresponds to the case $y=y'$ (which forces $s=s'$), and the term II corresponds to the case $y\neq y'$ (and so $s\neq s'$).

In the latter case we may set $a=s/s', b=s'$ and obtain, for $t\neq 0$,

(3.3)
$$\begin{aligned}II &= |E| q^{d-2} \textstyle\sum_{y,b\neq 0;\, a\neq 0,1} \chi(tb(1-a))E(y)E(ay) \\ &= -|E| q^{d-2} \textstyle\sum_{y,a\neq 1,0} E(y)E(ay).\end{aligned}$$

Thus,

$$\begin{aligned} |II(t)| &\leq |E|q^{d-2}\textstyle\sum_{y\in E\setminus\{(0,\ldots,0)\}}(|E\cap l_y|+1) \\ &\leq |E|^2q^{d-1}, \end{aligned} \tag{3.4}$$

since $|E\cap l_y|+1\leq q$ by virtue of the fact that each straight line contains exactly q points. The term $+1$ above has been added because in (2.3) above, the line l_y was defined away from the origin.

In the case $s=s'$ we get

$$I(t)=|E|q^{d-2}\sum_{s\neq 0;y}E(y)<|E|^2q^{d-1}. \tag{3.5}$$

It follows that for $t\neq 0$,

$$R^2(t)\leq -Q(t)+|E|^2q^{d-1},$$

with

$$Q(t)\geq 0.$$

Therefore, for $t\neq 0$ we have the bound (2.5),

$$|R(t)|\leq |E|q^{\frac{d-1}{2}}. \tag{3.6}$$

The same argument shows that

$$|R(0)|\leq |E|q^{\frac{d}{2}}.$$

3.3. **Proof of Corollary 2.4.** We now turn our attention to Corollary 2.4. The sufficient condition for $\Pi(E)\supseteq \mathbb{F}_q^*$ follows immediately from (3.2) and (3.6). Quite simply, it follows that $\nu(t)>0$ for all $t\neq 0$.

To address the statement (i) of the corollary, let us consider the case $d=2$ and $q=p^2$, where p is a power of a large prime. The higher-dimensional case follows similarly. Let a be a generator of the cyclic group $\mathbb{F}_q^*$. Then $a^{q-1}=1$ and a^{p+1} is the generating element for $\mathbb{F}_p^*$ since $p+1=\frac{q-1}{p-1}$.

Let A be a proper cyclic subgroup of $\mathbb{F}_q^*$ which properly contains $\mathbb{F}_p^*$. Let s be a divisor of $p+1$ and let the generating element of A be $\alpha=a^s$. Note that we are taking advantage of the fact that $\mathbb{F}_q^*$ is cyclic. Consider the unit circle

$$\{x\in\mathbb{F}_q^2: x_1^2+x_2^2=1\}$$

and its subset

$$C_p=\{x\in\mathbb{F}_p^2: x_1^2+x_2^2=1\}.$$

By elementary number theory (or Lemma 5.2), the cardinality of C_p is $p\mp 1$, depending on whether negative one is or is not a square in $\mathbb{F}_p^*$. Clearly, for any $u,v\in C_p$, $u\cdot v\in\mathbb{F}_p$. Let

$$E=\{tu: t\in A, u\in C_p\}. \tag{3.7}$$

For any $x,y\in E$, the dot product $x\cdot y$, if nonzero, will lie in A. Indeed, if $x=tu$, $y=\tau v$, according to (3.7), then

$$x\cdot y=t\tau(u\cdot v)\in A\cup\{0\},$$

since A contains $\mathbb{F}_p^*$. The cardinality of E is

$$|E|=\frac{p\mp 1}{2}|A|=\frac{p\mp 1}{2}\cdot\frac{q-1}{s},$$

where s is a divisor of $p+1$. Taking $s=2$ works and shows that less than half the elements of $\mathbb{F}_q^*$ may be realized as dot products determined by a set of size in excess of $\frac{1}{4}\cdot q^{\frac{3}{2}}$. In order to see that $\{x\cdot y : x,y\in E\}$ does not in general even contain a positive proportion of the elements of $\mathbb{F}_q$ if $|E|\ll q^{\frac{3}{2}}$, we need to produce a sequence of primes, or prime powers, such that $p+1$ has large divisors. We can do this using field extensions as follows.

Consider the family of prime powers

$$\{p^{2k+1} : k=1,2,\dots\}$$

and observe that

$$p+1 \mid p^{2k+1}+1.$$

This completes the construction demonstrating the claim (i). To take care of the higher-dimensional case, simply replace circles by spheres and the same argument goes through.

The claim (ii) of the corollary will follow immediately from the construction used in the proof of item (v) of Theorem 2.8 (see Section 5.5). On any sphere $\{x\in\mathbb{F}_q^d : x_1^2+\dots+x_d^2=r\}$, with $d=4m+3$, we can find a set E, with $|E|\gtrsim q^{\frac{d+1}{2}}$, such that the dot product $t=-r$ is not achieved.

4. Proof of the arithmetic results

4.1. **Proof of Theorem 2.5.** We may assume, without loss of generality, that A does not contain 0. Let $E=\underbrace{A^2+\dots+A^2}_{d \text{ times}}$. The proof of the first part of Theorem 2.5 follows instantly from the estimate (2.4). To prove the second part observe that

$$|E\cap l_y|\le |A| = |E|^{\frac{1}{d}}$$

for every $y\in E$. Using this, the estimate (2.2) implies, by the Cauchy-Schwarz inequality, that

$$|E|^4 = \left(\sum_t \nu(t)\right)^2 \le |\Pi(E)|\cdot\sum_t \nu^2(t), \tag{4.1}$$

that

$$|\{(x\cdot y : x,y\in E\}| \ge q\cdot\frac{|E|^2}{q^d\cdot|E|^{\frac{1}{d}}+|E|^2},$$

and, consequently, that

$$|\{x\cdot y : x,y\in E\}| \ge q\cdot\frac{C_1^{2-\frac{1}{d}}}{C_1^{2-\frac{1}{d}}+1}$$

if

$$|E|\ge C_1 q^{\frac{d}{2}+\frac{d}{2(2d-1)}}.$$

It follows that if

$$|A|\ge C_1^{\frac{1}{d}} q^{\frac{1}{2}+\frac{1}{2(2d-1)}},$$

then

$$|dA^2|\ge q\cdot\frac{C_1^{2-\frac{1}{d}}}{C_1^{2-\frac{1}{d}}+1},$$

as desired. This completes the proof of Theorem 2.5.

4.2. **Proof of the conditionally optimal arithmetic result (Theorem 2.6).** Once again throw zero out of A if it is there, and let $E = A \times A$. Using (2.2) we see that

$$\sum_t \nu^2(t) \leq |E|^4 q^{-1} + q^3|E| \sum_{k \neq (0,0)} |E \cap l_k| \left|\widehat{E}(k)\right|^2.$$

Now,

$$\begin{aligned} q^3|E| \textstyle\sum_{k\neq(0,0)} |E \cap l_k| \left|\widehat{E}(k)\right|^2 &\leq q^3|E| \cdot |E| \cdot \left|\widehat{E}(1,1)\right|^2 \\ &\quad + q^3|E| \textstyle\sum_{k\neq(0,0),(1,1)} |E \cap l_k| \left|\widehat{E}(k)\right|^2 \\ &\leq |E|^4 q^{-1} + C_2|E|^3. \end{aligned}$$

It follows that

$$\begin{aligned} |2A^2| &= |\{x \cdot y : x, y \in E\}| \\ &\geq \tfrac{|E|^4}{|E|^4 q^{-1} + C_2|E|^3} \\ &\geq q \cdot \tfrac{C_1}{2C_1 + C_2}, \end{aligned}$$

as desired.

5. Distances: Proofs of Theorems 2.7, 2.8 and 2.11

5.1. **Proof of Theorem 2.7.** We begin by proving the following lemma.

Lemma 5.1. *We say that $v \in \mathbb{F}_q^d$, $v \neq (0, \ldots, 0)$, is a null vector if $v \cdot v = 0$. If $d \geq 4$ is even, then there exist $\frac{d}{2}$ mutually orthogonal null vectors $v_1, \ldots, v_{\frac{d}{2}}$ in $\mathbb{F}_q^d$.*

To prove the lemma, suppose there exists an element $i \in \mathbb{F}_q$ such that $i^2 = -1$. Consider the collection of vectors

$$v_1 = (1, i, 0, 0, \ldots, 0, 0),\ v_2 = (0, 0, 1, i, \ldots, 0, 0), \ldots, v_{\frac{d}{2}} = (0, 0, \ldots, 0, 0, 1, i).$$

It follows immediately that

$$v_k \cdot v_l = 0$$

for every $k, l = 1, \ldots, \frac{d}{2}$.

If -1 is not a square, then from simple counting there exists a null vector

$$v_1 = (a, b, c, 0 \ldots, 0),$$

with all $a, b, c \in \mathbb{F}_q^*$. Suppose d is a multiple of 4. Then we may take the null vector

$$v_2 = (0, -c, b, a, \ldots, 0),$$

noting that this vector is orthogonal to v_1. In this same way we may now take the null vector

$$v_3 = (0, 0, 0, 0, a, b, c, 0, \ldots, 0),$$

and find a corresponding null vector v_4 which is orthogonal to v_3 as well as trivially orthogonal to v_1 and v_2. Continuing in this manner we obtain $\frac{d}{2}$ mutually orthogonal null vectors.

The proof will now be complete if we can also treat the case $d = 6$. In this case, let

$$v_1 = (a, b, c, 0, 0, 0),\ \ v_2 = (0, 0, 0, a, b, c),\ \text{where } a^2 + b^2 + c^2 = 0.$$

Consider two three-vectors

$$w_1 = (-b/c, a/c, 0) \text{ and } w_2 = (0, -c/a, b/a).$$

Let $s \in \mathbb{F}_q$ be such that

$$e_1 = w_1 + sw_2$$

satisfies $||e_1|| = 1$. Such an s exists, by the Lagrange theorem on quadratic forms (or can be verified by direct calculation).

Now consider a six-vector $v_3 = [e_1, w_1]$. By construction, v_3 is orthogonal to both v_1 and v_2. It is also a null vector, as $e_1 \cdot e_1 = 1$, while $w_1 \cdot w_1 = -1$.

This completes the proof of Lemma 5.1.

Let $d = 2m + 1$. Then from the above lemma there are m mutually orthogonal null vectors $v_1, \dots, v_m$, such that their dth coordinate is zero. Now let $A \subset \mathbb{F}_q$ be an arithmetic progression of length n and $u = (0, \dots, 0, 1)$. Consider the set

$$E = \{t_i v_i + au \text{ for } i = 1, \dots, m : t_i \in \mathbb{F}_q, a \in A\}.$$

We have

$$|E| = q^m \cdot |A| = q^m \cdot n.$$

For any $x, y \in E$ we have from orthogonality that

$$\|x - y\| = \|t_1 u_1 + av - t_2 u_2 - a' v_2\| = ||a - a'||,$$

so $|\Delta(E)| \leq 2n - 1$.

It follows that if we choose $2n = cq$, we have constructed, for any small c, a set E of $\frac{1}{2} c q^{\frac{d+1}{2}}$ generating fewer than cq distances. This completes the proof in the case $d \geq 5$.

If $d = 3$, and -1 is a square, take the null vector $v = (1, i, 0)$ and $u = (0, 0, 1)$. If -1 is not a square, take the null vector $v = (a, b, c)$ such that no entry can be zero, and let $u = (-b, a, 0)$. The proof then proceeds as above.

5.2. **Proof of Theorem 2.8, claim (i).** Since $E \subset S$,

$$\|x - y\| = (x - y) \cdot (x - y) = 2 - 2x \cdot y,$$

so counting distances on the sphere is the same as counting dot products.

Since now E is a subset of the sphere, it does not contain the origin and

$$|E \cap l_k| \leq 2.$$

Thus we conclude from the estimate (2.2) of Theorem 2.1 that

$$\begin{aligned} |E| q^{2d-1} \textstyle\sum_{k \neq (0,\dots,0)} |E \cap l_k| \left|\widehat{E}(k)\right|^2 &\leq 2|E| q^{2d-1} \textstyle\sum_{k \neq (0,\dots,0)} \left|\widehat{E}(k)\right|^2 \\ &\leq 2|E| q^{2d-1} q^{-d} \textstyle\sum_x E^2(x) \\ &= 2|E|^2 q^{d-1}. \end{aligned} \tag{5.1}$$

By application of the Cauchy-Schwarz inequality (4.1) we conclude that if $|E| \geq cq^{\frac{d}{2}}$, we have

$$|\Delta(E)| \geq Cq.$$

5.3. **Proof of the claim (iv).** The claim for $x \cdot y \neq 0$ follows immediately from Corollary 2.4, without requiring d to be odd. The case $x \cdot y = 0$ will be addressed further in Section 5.4.

5.4. **Proof of Theorem 2.8, claim (ii).** We now turn to the proof of (2.11). We will not distinguish between even and odd d until it becomes necessary. We proceed as in (3.2) in the proof of Corollary 2.4 by writing

$$\nu(t) = |E|^2 q^{-1} + R(t),$$

and we apply the Cauchy-Schwarz inequality to $R^2(t)$. This time, however, instead of dominating the sum over E by the sum over $\mathbb{F}_q^d$, we dominate the sum over E by the sum over the sphere S using the assumption that $E \subset S$. This yields

$$\begin{aligned} R^2(t) &\leq q^{-2}|E| \sum_{x\in S} \sum_{s,s'\neq 0} \sum_{y,y'\in E} \chi(sx\cdot y - s'x\cdot y')\chi(t(s'-s)) \\ &= q^{d-2}|E| \sum_{s,s'\neq 0} \chi(t(s'-s)) \sum_{y,y'\in E} \widehat{S}(s'y'-sy) \qquad (5.2) \\ &= I + II, \end{aligned}$$

where the term I corresponds to the case $s'y' = sy$. One of the keys to this argument is that since E is a subset of the sphere, $sy = s'y'$ can only happen if $y = \pm y'$ and $s = \pm s'$.

Lemma 5.2 below tells us that $\widehat{S}(0,\dots,0) = q^{-1}+$ lower order terms (unless $d = 2$), and it follows that

$$I \leq q^{d-2}|E|^2. \qquad (5.3)$$

To estimate the term II, we have to use the explicit form of the Fourier transform of the discrete sphere. For the reader's convenience we replicate one of the arguments in [12].

Lemma 5.2. *Let*

$$S_r = \{(x_1,\dots,x_d) \in \mathbb{F}_q^d : x_1^2 + \dots + x_d^2 = r\}.$$

Then for $k \in \mathbb{F}_q^d$,

$$\widehat{S}_r(k) = q^{-1}\delta(k) + K^d q^{-\frac{d+2}{2}} \sum_{j\in\mathbb{F}_q^*} \chi\left(\frac{\|k\|}{4j} + rj\right)\eta^d(-j), \qquad (5.4)$$

where the notation $\delta(k) = 1$ if $k = (0,\dots,0)$ and $\delta(k) = 0$ otherwise. The constant K equals ± 1 or $\pm i$, depending on q, and η is the quadratic multiplicative character (or the Legendre symbol) of $\mathbb{F}_q^*$.

5.4.1. *Proof of Lemma* 5.2. For any $k \in \mathbb{F}_q^d$, we have

$$\begin{aligned} \widehat{S}_r(k) &= q^{-d} \sum_{x\in\mathbb{F}_q^d} q^{-1} \sum_{j\in\mathbb{F}_q} \chi(j(\|x\| - r))\chi(-x\cdot k) \\ &= q^{-1}\delta(k) + q^{-d-1} \sum_{j\in\mathbb{F}_q^*} \chi(-jr) \sum_x \chi(j\|x\|)\chi(-x\cdot k) \qquad (5.5) \\ &= q^{-1}\delta(k) + K^d q^{-\frac{d+2}{2}} \sum_{j\in\mathbb{F}_q^*} \chi\left(\tfrac{\|k\|}{4j} + jr\right)\eta^d(-j). \end{aligned}$$

In the line before the last we have completed the square, changed j to $-j$, and used d times the Gauss sum

$$\sum_{c\in\mathbb{F}_q} \chi(jc^2) = \eta(j) \sum_{c\in\mathbb{F}_q} \eta(c)\chi(c) = \eta(j) \sum_{c\in\mathbb{F}_q^*} \eta(c)\chi(c) = K\sqrt{q}\,\eta(j), \qquad (5.6)$$

where $K = \pm i$ or ± 1, depending on q and $\eta(0) = 0$. See any standard text on finite fields for background and basic results about Gauss sums. Note that we have assumed that $\chi = \chi_1$ is the principal additive character of the field $\mathbb{F}_q$ (which means that for $t \in \mathbb{F}_q$, and $q = p^s$, where p is a prime, $\chi(t) = e^{\frac{2\pi i \mathrm{Tr}(t)}{p}}$, where $\mathrm{Tr} : \mathbb{F}_q \mapsto \mathbb{F}_p$ is the principal trace; see e.g. [15]). The specific choice of a principal character is of no consequence to the calculations in this paper.

We remark that for even d, the sum in the last line of (5.5) is the Kloosterman sum, while for odd d the presence of the quadratic character η would reduce it via the Gauss sum to a "cosine", which is nonzero only if $\theta^2 \equiv \frac{r\|k\|}{4}$ is a square in $\mathbb{F}_q^*$, in which case

$$\sum_{j \in \mathbb{F}_q^*} \chi\left(\frac{\|k\|}{4j} + jr\right) \eta(-j) = K\sqrt{q}\,\eta(-\|k\|^2)(\chi(2\theta) + \chi(-2\theta)). \tag{5.7}$$

We now return to the proof of (2.11). From now on, let K, K' stand for complex numbers of modulus 1 that may change from line to line. We now continue with the estimation of the term II in (5.2). Namely, we have

$$II = q^{d-2}|E| \sum_{y,y' \in E} \sum_{s,s' \in \mathbb{F}_q^*, s's' \neq sy} \widehat{S}(s'y' - sy)\chi(t(s' - s)) = III + IIII,$$

where the term III corresponds to the case the case $y = y'$, when $s \neq s'$. Then we have

$$III = q^{d-2}|E| \sum_{y \in E} \sum_{s,s' \in \mathbb{F}_q^*, s \neq s'} \widehat{S}((s' - s)y)\chi(t(s' - s)).$$

Observe that $s' - s$ runs through each value in $\mathbb{F}_q^*$ exactly $q - 1$ times. Also, $||y|| = 1$ since $E \subset S$. Therefore, using Lemma 5.4, we have

$$\begin{aligned} III &= Kq^{d-2}|E| \textstyle\sum_{y \in E}(q-1)q^{-\frac{d+2}{2}} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\frac{s^2}{4j} + ts + j\right)\eta^d(j) \\ &= Kq^{d-2}|E| \textstyle\sum_{y \in E}(q-1)\cdot q^{-\frac{d+2}{2}} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\frac{(s+2jt)^2}{4j} - jt^2 + j\right)\eta^d(j) \\ &= K\tfrac{q-1}{q} q^{\frac{d-4}{2}}|E| \textstyle\sum_{y \in E} \sum_{j \in \mathbb{F}_q^*} \chi(j - jt^2)\eta^d(j)[-\chi(jt^2) + K'\sqrt{q}\eta(j)], \end{aligned} \tag{5.8}$$

where the last line follows by (5.6).

We now consider the case $t^2 = \|y\| = 1$. We have

$$III_{t^2=1} \approx q^{\frac{d-4}{2}}|E| \sum_{y \in E} \sum_{j \in \mathbb{F}_q^*} \eta^d(j)[-\chi(j) + K\sqrt{q}\eta(j)].$$

Since $\sum_{j \in \mathbb{F}_q^*} \eta(j) = 0$, the worst case scenario occurs when d is odd. Then the summation in j contributes an extra factor $q - 1$ to $K\sqrt{q}$ in the last bracket. If d is even, then the summation in j is the Gauss sum, which is smaller by the factor of $\sqrt{q}$. In either case, we have

$$|III_{t^2=1}| \leq 2q^{\frac{d-1}{2}}|E|^2. \tag{5.9}$$

If $t^2 \neq 1$, the estimate (5.9) improves by the factor $\sqrt{q}$, as the worst case scenario is now when d is even, and it only contributes a Gauss sum to the term $K\sqrt{q}$:

$$\sum_{j\in\mathbb{F}_q^*} \chi(j-jt^2)\eta^d(j)[-\chi(jt^2)+K\sqrt{q}\eta(j)]. \tag{5.10}$$

Observe, however, that in either case, for $d \geq 2$ the estimate for the term III is majorized by (5.3).

Finally, let us consider the term $IIII$:

$$IIII = q^{d-2}|E| \sum_{y,y'\in E, y\neq y'} \sum_{s,s'\in\mathbb{F}_q^*} \widehat{S}(s'y'-sy)\chi[t(s'-s)]. \tag{5.11}$$

Our goal is to prove the following estimate:

$$|IIII = IIII(t)| \ \lesssim \ q^{\frac{d-4}{2}}|E|^3 + q^{\frac{d-2}{2}}|E| \sup_{\tau\in\mathbb{F}_q} |R(\tau)|, \tag{5.12}$$

and we are able to do it only for even values of d. (For odd d the estimate will definitely be worse by $\sqrt{q}$ for $t^2 = 1$ and seems to be highly nontrivial for other values of t; see (5.19) below.) Note that we can always write $\sup_{\tau\in\mathbb{F}_q} \nu(\tau)$ instead of $\sup_{\tau\in\mathbb{F}_q} |R(\tau)|$, as the regular term $\frac{|E|^2}{q}$ can be absorbed into the first term in (5.12).

We verify (5.12) below and will now show how it suffices to complete the proof of (2.11). Indeed, assuming (5.12) and bringing in the estimate (5.3), which dominated the terms I, III, we conclude that for all t,

$$R^2(t) \ \lesssim \ q^{d-2}|E|^2 + q^{\frac{d-4}{2}}|E|^3 + q^{\frac{d-2}{2}}|E| \sup_{\tau\in\mathbb{F}_q} |R(\tau)|,$$

which implies that the same estimate holds for $\sup_{\tau\in\mathbb{F}_q} R^2(\tau)$.

Assuming that for some large enough C we have $Cq^{\frac{d}{2}} \leq |E|$ clearly implies that now

$$|R(t)| \ \leq \ \frac{100}{\sqrt{C}}\frac{|E|^2}{q}, \quad \forall t \in \mathbb{F}_q,$$

where the constant 100 is basically to majorize the number of cases that have been considered. For odd d the last two terms in the latter estimate for R are worse by the factor $\sqrt{q}$, which implies the estimate (3.6) for all t, thus the claim (ii) of Theorem 2.8. As for even d, every dot product $t \in \mathbb{F}_q$ occurs and the claim (iv) of Theorem 2.8 follows, provided that we can demonstrate (5.12).

5.4.2. *Finale of the proof of claim (ii) – the estimate (*5.12*).* In the estimates that follow we write

$$\sum_{y,y'} \quad \text{instead of} \quad \sum_{y,y'\in E, y\neq y'}.$$

Let us first extend the summation in (5.11) from $s' \in \mathbb{F}_q^*$ to $s' \in \mathbb{F}_q$. If we do so, it follows from Lemma 5.4 that we pick up the following term T to $IIII$:

$$\begin{aligned} T &= q^{d-2}|E| \sum_{y,y'} \sum_{s \in \mathbb{F}_q^*} \widehat{S}(sy)\chi(ts) \\ &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\tfrac{s^2}{4j} + ts + j\right) \eta^d(j) \\ &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*} \chi\left(\tfrac{(s+2jt)^2}{4j} - jt^2 + j\right) \eta^d(j) \\ &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{j \in \mathbb{F}_q^*} \chi(j - jt^2)\eta^d(j)[-\chi(jt^2) + K'\sqrt{q}\eta(j)]. \end{aligned}$$

The analysis of the summation in j now in essence replicates that for the term III; see (5.8)–(5.10). If $t^2 \neq 1$ and d is even, using the Gauss sum formula (5.6) we obtain

$$|T| \ \leq \ 2q^{\frac{d-4}{2}}|E|^3, \tag{5.13}$$

which improves by the factor $\sqrt{q}$ if d is odd. If $t^2 = 1$, for even d, the term T satisfies a better (by a factor q) estimate than (5.13). However, for odd d we would only get $|T| \leq q^{\frac{d-3}{2}}|E|^3$, which would not give an improvement over the bounds we already have in (3.6). Hence, up to now, the only case we are not able to handle is odd d and $t^2 = 1$.

Thus we will further attempt to establish (5.12) for the quantity X, which equals $IIII$, wherein the summation in s' has been extended over the whole field $\mathbb{F}_q$. Using Lemma 5.4 we have, after changing s' to $-s'$, and using $\|y\| = \|y'\| = 1$:

$$X = Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*, s' \in \mathbb{F}_q} \eta^d(j)\chi\left(\frac{s^2 + 2(y \cdot y')ss' + s'^2 + 4tj(s+s')}{4j} + j\right). \tag{5.14}$$

We complete the square under χ as follows:

$$s^2 + 2(y \cdot y')ss' + s'^2 + 4tj(s+s') = (s+s')^2 + 4tj(s+s') + 2\alpha s'(s+s'-s'),$$

where $\alpha = \alpha(y,y') = y \cdot y' - 1$, and we shall further analyze the possibilities $\alpha \neq 0, -2$ separately: they occur when $y \cdot y' = \pm 1$, respectively.

We rewrite the latter quadratic form as

$$[(s+s') + (2tj + \alpha s')]^2 - 2\alpha s'^2 - (2tj + \alpha s')^2.$$

We now have a new variable $c = (s+s') + (2tj + \alpha s')$, which is in $\mathbb{F}_q$. Since (5.14) is symmetric with respect to s and s', we can assume that, in fact, $s \in \mathbb{F}_q$, $s' \in \mathbb{F}_q^*$, so for each s', j the change $s \mapsto c$ is nondegenerate. Changing the notation from $-s'$ to s we therefore have, using the Gauss sum formula,

$$\begin{aligned} X &= Kq^{\frac{d-6}{2}}|E| \sum_{y,y'} \sum_{s,j \in \mathbb{F}_q^*, c \in \mathbb{F}_q} \eta^d(j)\chi\left(\tfrac{c^2 - (2\alpha + \alpha^2)s^2}{4j} + t\alpha s + j(1-t^2)\right) \\ &= X_1 + X_{-1} + X', \end{aligned} \tag{5.15}$$

where X_1 has only summation in y, y' such that $y \cdot y' = 1$ ($\alpha = 0$), X_{-1} has only summation in y, y' such that $y \cdot y' = -1$ ($\alpha = -2$), and X' includes the rest of $y, y' \in E$.

Observe that in either case we already have a Gauss sum in c, so we write

(5.16)
$$X' = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'\neq\pm 1} \sum_{s,j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi\left(\frac{-a\left(s-\frac{2jt\alpha}{a}\right)^2}{4j} + j\left(\frac{t^2\alpha}{2+\alpha}+(1-t^2)\right)\right),$$

provided that $a = 2\alpha+\alpha^2 \neq 0$.

Before we proceed with the main term X', let us deal with the cases $\alpha = 0, -2$ which would make the completion of the square in the transition from (5.15) to (5.16) incorrect.

If $\alpha = 0$, we confront the sum

$$X_1 = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'=1} \sum_{s,j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi(j(1-t^2)).$$

If d is even, the worst case scenario is $t^2 \neq 1$, when the sum in s and Gauss sum in j contribute the factor $q^{3/2}$. Hence

$$|X_1| \leq 2q^{\frac{d-2}{2}}|E| \sup_{\tau} \nu(\tau), \quad \text{for even } d, \tag{5.17}$$

in accordance with (5.12). If d is odd, the same, or in fact, better bound holds unless $t^2 = 1$, when (5.17) gets worse by the factor $\sqrt{q}$.

If $\alpha = -2$, we analyze the sum

$$X_{-1} = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'=-1} \sum_{s,j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi(j(1-t^2)-2ts).$$

If d is even, X_{-1} is still bounded by (5.17) and the worst case scenario now is $t = 0$; if d is odd, the bound is better than (5.17) by the factor $\sqrt{q}$.

Finally, we turn to X', the case $a \neq 0$, and once again, the only situation we have not been able to handle so far is d odd and $t^2 = 1$.

Now taking advantage of the Gauss sum in s in (5.16) we have

$$\begin{aligned} X' &= Kq^{\frac{d-5}{2}}|E| \textstyle\sum_{y\cdot y'\neq\pm 1} \sum_{j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi\left(j\left(\frac{t^2\alpha}{2+\alpha}+(1-t^2)\right)\right) \\ &\qquad \times \left[-\chi\left(-j\tfrac{t^2\alpha}{2+\alpha}\right) + K'\sqrt{q}\eta(a)\eta(j)\right] \\ &= X_1' + X_2', \end{aligned}$$

according to the two terms in the last bracket.

We have

$$X_1' = Kq^{\frac{d-5}{2}}|E| \sum_{y\cdot y'\neq\pm 1} \sum_{j\in\mathbb{F}_q^*} \eta^{d+1}(j)\chi(j(1-t^2)).$$

For even d, the worst case scenario occurs when $t^2 \neq 1$, the Gauss sum in j then leads to X_1' to be dominated by the first term in (5.12). The latter bound will get worse by the factor $\sqrt{q}$ only if d is odd and $t^2 = 1$. For the quantity X_2' we obtain:

(5.18)
$$\begin{aligned} X_2' &= Kq^{\frac{d-4}{2}}|E| \textstyle\sum_{y\cdot y'\neq\pm 1} \eta(a) \sum_{j\in\mathbb{F}_q^*} \eta^d(j)\chi\left(\left(1-\frac{2}{2+\alpha}t^2\right)j\right) \\ &= Kq^{\frac{d-4}{2}}|E| \textstyle\sum_{y\cdot y'\neq\pm 1} \eta[(y\cdot y')^2-1] \sum_{j\in\mathbb{F}_q^*} \eta^d(j)\chi\left(\left(1-\frac{2}{y\cdot y'+1}t^2\right)j\right). \end{aligned}$$

There are two cases here: $y \cdot y' = 2t^2 - 1$ and otherwise. First consider the latter case. Then if d is even, X_2', subject to this extra constraint, satisfies the estimate (5.12), as the summation in j simply yields -1. If d is odd, however, there is a major problem, as then we have

(5.19)
$$q^{\frac{d-4}{2}}|E| \sum_{y\cdot y' \neq 2t^2-1,\pm 1} \eta((y\cdot y')^2-1) \sum_{j\in \mathbb{F}_q^*} \eta^d(j) \chi\left(\left(1-\tfrac{2}{y\cdot y'+1}t^2\right)j\right)$$
$$= Kq^{\frac{d-3}{2}}|E| \sum_{y\cdot y' \neq 2t^2-1,\pm 1} \eta((y\cdot y')-1)\eta((y\cdot y')+1-2t^2).$$

It follows that to improve on the trivial bound $q^{\frac{d-3}{2}}|E|^3$ one would have to establish a cancellation in the multiplicative character sum in (5.19).

We finish by adding the constraint $y \cdot y' = 2t^2 - 1$ to X_2' in (5.18). Dealing with this does not represent any difficulty. For even d we have

$$q^{\frac{d-4}{2}}|E| \left| \sum_{\pm 1 \neq y\cdot y' = 2t^2-1} \eta[(y\cdot y')^2-1] \sum_{j\in\mathbb{F}_q^*} \eta^d(j) \right| \leq q^{\frac{d-2}{2}}|E| \sup_{\tau\in\mathbb{F}_q} \nu(\tau),$$

and zero in the right-hand side for odd d. This proves (5.12), and (2.11) follows.

5.5. **Proof of Theorem 2.8, optimality claims (iii) and (v).** We establish (2.14) as the estimate (2.12) follows immediately from the same construction.

5.6. **Construction in the case $d \neq 5$.** Suppose that $\mathbb{F}_q$ does not contain $i = \sqrt{-1}$. Let

$$S^2 = \{x \in \mathbb{F}_q^3 : x_1^2 + x_2^2 + x_3^2 = 1\},$$

and let Z_2 denote the maximal subset of S^2 such that $Z_2 \cap (-Z_2) = \emptyset$. Then if $u, v \in S^2$, then $u \cdot v = -1$ if and only if $u = -v$. To see this, without loss of generality let $v = (0, 0, 1)$. Then the condition

$$u \cdot v = -1$$

reduces to

$$u_3 = -1$$

and

$$u_1^2 + u_2^2 = 0. \tag{5.20}$$

Since, by assumption, $\mathbb{F}_q$ does not contain $\sqrt{-1}$, (5.20) can only happen if $u_1 = u_2 = 0$, and so $u = -v$. Since $Z_2 \cap (-Z_2) = \emptyset$, the condition $u \cdot v = -1$ in Z_2 is never satisfied.

Let $d = 2k + 1$ with $k \geq 3$. Let H denote subspace of $\mathbb{F}_q^{2k-2}$ generated by the mutually orthogonal null-vectors given by Lemma 5.1. Let

$$E = Z_2 \times H.$$

It follows that

$$|E| \approx q^2 \cdot q^{k-1} = q^{k+1} = q^{\frac{d+1}{2}}.$$

Let (x', x'') and (y', y'') be elements of E. Then

$$(x', x'') \cdot (y', y'') = x' \cdot y' \neq -1.$$

Moreover,

$$||(x', x'')|| = ||x'|| + ||x''|| = ||x'|| = 1,$$

so $E \subset S^{2k}$, where

$$S^{2k} = \{x \in \mathbb{F}_q^{2k+1} : x_1^2 + \cdots + x_{2k+1}^2 = 1\}.$$

This completes the construction in the case $d \neq 5$.

5.7. **Construction in the case $d = 5$.** Let

$$u = (a, b, c, 0, 0) \text{ where } a^2 + b^2 + c^2 = 0.$$

Let

$$v = (-b/c, a/c, 0, 0, 0) \text{ and } w = (0, -c/a, b/a, 0, 0).$$

Let $s \in \mathbb{F}_q$ be such that

$$e = v + sw$$

satisfies

$$||e|| = c^2 \text{ for some } c \in \mathbb{F}_q^*.$$

The existence of such a c is verified by a direct calculation. Now let $e' = \frac{e}{c}$, which results in $||e'|| = 1$.

Observe by a direct calculation that

$$u \cdot e = 0 \text{ for all } s \in \mathbb{F}_q.$$

Let Z_2 be as above and let O denote the orthogonal transformation that maps

$$\{(x_1, x_2, x_3, 0, 0) : x_j \in \mathbb{F}_q\}$$

to the three-dimensional subspace of $\mathbb{F}_q^5$ spanned by e', $(0, 0, 0, 1, 0)$ and $(0, 0, 0, 0, 1)$. Let Z_2' denote the image of Z_2 under O.

Define

$$E = \{tu + Z_2' : t \in \mathbb{F}_q\}.$$

Then $|E| \approx q^3$ and for any $t, t' \in \mathbb{F}_q$ and $z, z' \in Z_2'$,

$$\begin{aligned}(tu + z) \cdot (t'u + z') &= tt'u \cdot u + tu \cdot z' + t'u \cdot z + z \cdot z' \\ &= z \cdot z' \neq -1\end{aligned}$$

by construction. This completes the construction in the case $d = 5$.

5.8. **Proof of the conditionally optimal result (Theorem 2.11).** Once again we use the estimate (2.2), which tells us that

$$\sum_t \nu^2(t) \leq |E|^4 q^{-1} + |E| q^{2d-1} \sum_{k \neq (0,\ldots,0)} |E \cap l_k| \left|\widehat{E}(k)\right|^2.$$

Now,

$$|E| q^{2d-1} \sum_{k \neq (0,\ldots,0)} |E \cap l_k| \left|\widehat{E}(k)\right|^2 \leq 2|E| q^{2d-1} \sum_{k \in C(E)} \left|\widehat{E}(k)\right|^2,$$

where

$$C(E) = \bigcup_{t \in \mathbb{F}_q} tE.$$

Furthermore,

(5.21)
$$\begin{aligned} |E|q^{2d-1}\sum_{k\in C(E)}\left|\widehat{E}(k)\right|^2 &= |E|q^{2d-1}q^{-2d}\sum_{y,y'\in E}\sum_{k\in C(E)}\chi((y'-y)\cdot k) \\ &= |E|q^{-1}\sum_{y,y'\in E}\sum_{t}\sum_{x\in E}\chi((y-y')\cdot tx) \\ &= |E|^3+|E|\sum_{(y-y')\cdot x=0;y\neq y'}E(x)E(y)E(y'). \end{aligned}$$

Since E is assumed to be uniformly distributed,

$$\sum_{(y-y')\cdot x=0} E(x)\leq C|E|q^{-1};$$

plugging this into (5.21) we obtain $|E|^4q^{-1}$. Using (4.1) once again we complete the proof. Observe that the assumption that $|E|\geq Cq$ is implicit in the uniform distributivity assumption.

References

[1] N. Alon and M. Krivelevich, *Constructive bounds for a Ramsey-type problem*, Graphs and Combinatorics **13** (1997), 217-225. MR1469821 (98h:05136)

[2] J. Bourgain, A. A. Glibichuk and S. V. Konyagin. *Estimates for the number of sums and products and for exponential sums in fields of prime order*. J. London Math. Soc. (2) **73** (2006), 380–398. MR2225493 (2007e:11092)

[3] J. Bourgain, N. Katz and T. Tao. *A sum-product estimate in finite fields, and applications*. Geom. Funct. Anal. **14** (2004), 27–57. MR2053599 (2005d:11028)

[4] E. Croot. *Sums of the Form* $1/x_1^k+\cdots+1/x_n^k$ *modulo a prime*. Integers **4** (2004). MR2116005 (2005i:11028)

[5] B. Erdoğan. *A bilinear Fourier extension theorem and applications to the distance set problem*. Int. Math. Res. Not. **23** (2005), 1411–1425. MR2152236 (2006h:42020)

[6] P. Erdős. *On sets of distances of n points*. Amer. Math. Monthly **53** (1946), 248–250. MR0015796 (7:471c)

[7] M. Garaev. *The sum-product estimate for large subsets of prime fields*, Proc. Amer. Math. Soc. **136** (2008), 2735–2739. MR2399035 (2009e:11043)

[8] A. A. Glibichuk. *Combinatorial properties of sets of residues modulo a prime and the Erdős-Graham problem*. Mat. Zametki **79** (2006), 384–395; translation in: Math. Notes **79** (2006), 356–365. MR2251362 (2007e:11120)

[9] A. Glibichuk and S. Konyagin. *Additive properties of product sets in fields of prime order*. Centre de Recherches Mathématiques, Proceedings and Lecture Notes, 2006. MR2359478 (2009a:11054)

[10] D. Hart and A. Iosevich. *Sums and products in finite fields: an integral geometric viewpoint*, Contemporary Mathematics: Radon transforms, geometry, and wavelets **464** (2008). MR2440133 (2009m:11032)

[11] D. Hart, A. Iosevich and J. Solymosi. *Sum-product theorems in finite fields via Kloosterman sums*. Int. Math. Res. Notices (2007) Vol. 2007, article ID rmn007, 14 pages.

[12] A. Iosevich and M. Rudnev. *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. **359** (2007), 6127–6142. MR2336319 (2008k:11130)

[13] A. Iosevich, M. Rudnev and I. Uriarte-Tuero. *Theory of dimension for large discrete sets and applications*. Preprint, arxiv.org, 2007.

[14] N. H. Katz and C.-Y. Shen. *Garaev's Inequality in finite fields not of prime order*. Online J. Anal. Comb. No. 3 (2008), Art. 3, 6 pp. MR2375606 (2008k:12004)

[15] R. Lidl and H. Niederrieter. *Finite Fields*. Encyclopedia of Mathematics and its Applications **20**, Addison–Wesley 1983. MR746963 (86c:11106)

[16] J. Matousek. *Lectures on Discrete Geometry*, Graduate Texts in Mathematics. Springer **202**, 2002. MR1899299 (2003f:52011)

[17] P. Mattila. *Spherical averages of Fourier transforms of measures with finite energy; dimension of intersections and distance sets.* Mathematika **34** (2) (1987), 207–228. MR933500 (90a:42009)
[18] E. Stein. *Harmonic Analysis*. Princeton University Press, 1993. MR1232192 (95c:42002)
[19] T. Tao and V. Vu. *Additive Combinatorics*. Cambridge University Press, 2006. MR2289012 (2008a:11002)
[20] V. Vu. Sum-product estimates via directed expanders. Math. Res. Lett. **15** (2008), no. 2, 375–388. MR2385648 (2009e:11023)
[21] A. Weil. *On some exponential sums*. Proc. Nat. Acad. Sci. U.S.A. **34** (1948), 204–207. MR0027006 (10:234e)

Department of Mathematics, Rutgers University, 110 Frelinghuysen Road, Piscataway, New Jersey 08854-8019

Department of Mathematics, University of Rochester, Hylan 909, Rochester, New York 14627

Department of Mathematics, Michigan State University, East Lansing, Michigan 48824

School of Mathematics, University of Bristol, University Walk, Bristol, BS8 1TW England