Erdös distance problem in vector spaces over finite fields

A. Iosevich* and M. Rudnev†

January 25, 2006

Abstract

We study the Erdös/Falconer distance problem in vector spaces over finite fields. Let $\mathbb{F}_q$ be a finite field with q elements and take $E \subset \mathbb{F}_q^d$, $d \geq 2$. We develop a Fourier analytic machinery, analogous to that developed by Mattila in the continuous case, for the study of distance sets in $\mathbb{F}_q^d$ to provide estimates for minimum cardinality of the distance set $\Delta(E)$ in terms of the cardinality of E. Bounds for Gauss and Kloosterman sums play an important role in the proof.

Contents

The work was partly supported by the grant DMS02-45369 from the National Science Foundation, the National Science Foundation Focused Research Grant DMS04-56306, and the EPSRC grant GR/S13682/01.

AMS subject classification 11T, 42B, 52C

*University of Missouri, Columbia MO, 65211 USA, iosevich@math.missouri.edu

†University of Bristol, Bristol BS8 1TW UK, m.rudnev@bris.ac.uk

1 Introduction

Finite field analogs of classical problems in harmonic analysis, geometric measure theory and combinatorics have received much recent attention due the relative technical transparency afforded by the discrete setting and the presence of fascinating arithmetic considerations. See, for example, [23], [3], [17] and the references contained therein for the description of these efforts. In this paper we investigate the finite field analog of the Erdös/Falconer distance problems and develop the Fourier analytic machinery to study the problem. This machinery, while analogous in many respects to its Euclidean counterpart, exhibits some interesting new features forced upon the problem by number theoretic issues. We wish to stress that the main purpose of this paper is to introduce the relevant number theoretic machinery in the context of distance sets in a straightforward and relatively self-contained way.

In the Euclidean setting, the Erdös distance conjecture says that if E is a finite subset of $\mathbb{R}^d$, $d \geq 2$, then

$$\#\Delta_{\mathbb{R}^d}(E) \gtrapprox (\#E)^{\frac{d}{2}}, \tag{1.1}$$

where

$$\Delta_{\mathbb{R}^d} = \{|x-y| : x, y \in E\},$$

and

$$|x-y|^2 = (x_1-y_1)^2 + \cdots + (x_d-y_d)^2.$$

Here, and throughout the paper, $X \lesssim Y$ means that there exists $C > 0$ such that $X \leq CY$, $X \gtrsim Y$ means $Y \lesssim X$, and $X \approx Y$ if both $X \lesssim Y$ and $X \gtrsim Y$. Besides, $X \lessapprox Y$ ($X \gtrapprox Y$) means that for every $\epsilon > 0$ there exists $C_\epsilon > 0$ such that $X \leq C_\epsilon q^\epsilon Y$ ($X \geq C_\epsilon q^{-\epsilon} Y$), where q is a large controlling parameter. On occasion it will be necessary to emphasize the role of constants and in such cases we will introduce constants explicitly.

See, for example, [13] for the description of the Erdös distance problem in Euclidean space and references to recent results. We mention in passing that the Erdös distance conjecture is not solved in any dimension, in Euclidean or any other setting. The best known result in the Euclidean plane is due to Katz and Tardos ([11]) who prove that

$$\#\Delta_{\mathbb{R}^2}(E) \gtrsim (\#E)^{\approx .86}.$$

In this paper we study the Erdös distance problem in vector spaces over finite fields. This problem was recently addressed by Tao ([21]) who also relates it to some other open questions in combinatorics.

Let $\mathbb{F}_q$ denote the finite field with q elements, and let $\mathbb{F}_q^d$ denote the d-dimensional vector space over this field. Let $E \subset \mathbb{F}_q^d$, $d \geq 2$. Then the analog of the classical Erdös distance problem is to determine the smallest possible cardinality of the set

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

viewed as a subset of $\mathbb{F}_q$.

In the finite field setting, the estimate (1.1) cannot hold without further restrictions. To see this, let $E = \mathbb{F}_q^d$. Then $\#E = q^d$ and $\#\Delta(E) = q$. Furthermore, an interesting feature of the Erdös distance problem in the finite field setting is the existence of non-trivial spheres of 0 radius. These are sets of the form $\{x \in \mathbb{F}_q^d : x_1^2 + x_2^2 + \cdots + x_d^2 = 0\}$ and several assumptions in the statements of results below are there precisely to deal with issues created by the presence of this object. For example, suppose -1 is a square in $\mathbb{F}_q$. Using spheres of radius 0 one can show, in even dimensions, that there exists a set of cardinality precisely $q^{\frac{d}{2}}$ such that all the

distances, $(x_1-y_1)^2+\cdots+(x_d-y_d)^2$ are 0. See Example 4.4 below. What's more, suppose $\mathbb{F}_q$ is a finite field, such that $q=p^2$, where p is a prime. Then $E=\mathbb{Z}_p^d$ is naturally embedded in $\mathbb{F}_p^d$, has cardinality $q^{\frac{d}{2}}$, and determines only $\sqrt{q}$ distances. With these examples as our guide, we are led to the following conjecture.

Conjecture 1.1. *Let $E\subset\mathbb{F}_q^d$ of cardinality $\geq Cq^{\frac{d}{2}}$, with C sufficiently large. Then*

$$\#\Delta(E)\gtrapprox q.$$

In view of the above mentioned examples, it is tempting to formulate the following question.

Question 1.2. Is it true that in Conjecture 1.1 it suffices to take any $C>1$ (for q large enough)?

In order to see the sharpness of the exponents in Conjecture 1.1, consider the following construction. Let $\mathbb{F}_q=\mathbb{Z}_q$, where q is a prime. Let $d=2$ and let $E=\{x: x_j=0,1,\ldots,\left[\frac{\sqrt{q}}{2}\right]\}$. Then, by the well-known result in the Euclidean case (see e.g. [13]), $\#\Delta(E)\approx\frac{q}{\sqrt{\log(q)}}$.

A Euclidean plane argument due to Erdös ([5]) can be applied to the finite field set-up under the assumption of Conjecture 1.1 to show that if $d=2$, then

$$\#\Delta(E)\gtrsim(\#E)^{\frac{1}{2}}. \tag{1.2}$$

This result was improved by Bourgain, Katz and Tao ([3]) who showed using intricate incidence geometry that for every $\epsilon>0$, there exists $\delta>0$, such that if $\#E\lesssim q^{2-\epsilon}$, then

$$\#\Delta(E)\gtrsim q^{\frac{1}{2}+\delta}.$$

The relationship between ϵ and δ in the above argument is difficult to determine. The results of this paper clarify the nature of the exponents suggested by the theorem of Bourgain/Katz/Tao and apply to higher dimensions, where matters are more subtle in the context of vector spaces over finite fields because intersection of analogs of spheres in $\mathbb{F}_q^d$ may be quite complicated, and the standard dimensional induction in $\mathbb{R}^d$ argument (see e.g. [1]) that allows one to bootstrap the estimate (1.2) into the estimate

$$\#\Delta_{\mathbb{R}^d}(E)\gtrsim(\#E)^{\frac{1}{d}} \tag{1.3}$$

does not immediately go through. We establish the finite field analog of the estimate (1.3) below using Fourier analytic methods and number theoretic properties of Kloosterman sums.

Another way of thinking of Conjecture 1.1 is in terms of the Falconer distance conjecture ([6]) in the Euclidean setting which says that if the Hausdorff dimension of a set in $\mathbb{R}^d$ exceeds $\frac{d}{2}$, then the Lebesgue measure of the distance set is positive. Conjecture 1.1 implies that if the size of the set is greater than $q^{\frac{d}{2}}$, then the distance set contains a positive proportion of all the possible distances, an analogous statement.

As we have indicated above, methods of this paper are strongly motivated by the Falconer conjecture. In particular, a significant part of this paper is dedicated to the derivation of the finite field analog of Fourier theory for distance sets initially developed in the continuous setting by Falconer ([6]) and Mattila ([14]). See also some recent progress on this problem due to Bourgain ([2]), Erdoğan ([4]) and Wolff ([23]). The best currently known result is due to Erdoğan ([4]) and Wolff ([23]) who proved that the Lebesgue measure of the distance set is positive provided that the Hausdorff dimension of the set exceeds $\frac{d}{2}+\frac{1}{3}$. The authors have

recently shown ([9]) that for a class of measures arising as thickenings of well-distributed sets in $\mathbb{R}^d$, the exponent $\frac{d}{2}+\frac{1}{3}$ can be improved to $\frac{d}{2}+\frac{d}{4d-2}$. Note that Theorem 1.3 below mainly corresponds to the exponent $\frac{d}{2}+\frac{1}{2}$, proved in the continuous case by Falconer ([6]). The proof in the finite field case is more difficult and involves non-trivial number theory, mainly hidden in the known estimates for Kloosterman sums. There is a reasonable chance that uniform distribution estimates obtained for Kloosterman sums by Katz ([10]), Niederreiter ([18]) and others can be used to improve the results of this paper. We hope to address this issue in a subsequent paper.

1.1 Acknowledgements

The authors wish to thank M. B. Erdoğan for several useful remarks about the paper. The authors are also grateful to D. Edidin and S. Lev for suggesting various versions of the construction used in Example 4.4.

1.2 Statement of results

1.2.1 Analog of Erdös, Moser and Falconer's results

Historically, the first result on the Falconer distance conjecture ([6]) says that if the Hausdorff dimension of a set in $\mathbb{R}^d$, $d \geq 2$, is greater than $\frac{d+1}{2}$, then the Lebesgue measure of the Euclidean distance set is positive. The first result on the Erdös distance problem ([5]) is given by (1.2), and the second result in that direction, due to Moser ([16]), says that if E is a finite subset of $\mathbb{R}^2$, then $\#\Delta_{\mathbb{R}^2}(E) \gtrsim (\#E)^{\frac{2}{3}}$. Our first result is the finite field analog of these basic results.

Theorem 1.3. *Let $E \subset \mathbb{F}_q^d$ such that $\#E \gtrsim Cq^{\frac{d}{2}}$ for C sufficiently large. Then*

$$\#\Delta(E) \gtrsim \min\left\{q, \frac{\#E}{q^{\frac{d-1}{2}}}\right\}.$$

In particular, $\#\Delta(E) \gtrsim q$ if $\#E \gtrsim q^{\frac{d+1}{2}}$, from which it follows that if $\#E \approx q^{\frac{d+1}{2}}$, then $\#\Delta(E) \gtrsim (\#E)^{\frac{2}{d+1}}$, thus clarifying the nature of the exponents in the Bourgain/Katz/Tao result mentioned in the introduction and extending it to higher dimensions for the given range of exponents. This conclusion can also be viewed as a finite field analog of a result in the Euclidean setting due to Falconer ([6]) who proved that the distance set determined by a subset of $\mathbb{R}^d$, $d \geq 2$, of Hausdorff dimension greater than $\frac{d+1}{2}$ has positive Lebesgue measure.

Similarly, if $\#E \geq Cq^{\frac{d}{2}}$, with a sufficiently large C, then $\#\Delta(E) \gtrsim (\#E)^{\frac{1}{d}}$, thus establishing (1.3) in this range of exponents.

By modifying the proof of Theorem 1.3 slightly, we obtain the following stronger conclusion.

Theorem 1.4. *Let $E \subset \mathbb{F}_q^d$ such that $\#E \geq Cq^{\frac{d+1}{2}}$ for a sufficiently large constant C. Then for every $t \in \mathbb{F}_q$ there exist $x, y \in E$ such that $|x-y|^2 = t$. In other words, every distance is achieved.*

This result is analogous to the result in the Euclidean setting due to Mattila and Sjölin ([15], see also [19]), which says that if the Hausdorff dimension of a set E is greater than $\frac{d+1}{2}$, then the distance set is continuous with respect to the Lebesgue measure.

1.2.2 Analog of Mattila's circular average machinery

In the Euclidean setting, the key object used to study the Falconer distance conjecture is the spherical average

$$\int_{S^{d-1}} |\widehat{\mu}(t\omega)|^2 d\omega, \tag{1.4}$$

where μ is a Borel measure on the set under consideration, and the Mattila integral

$$\int_0^\infty \left(\int_{S^{d-1}} |\widehat{\mu}(t\omega)|^2 d\omega \right)^2 t^{d-1} dt. \tag{1.5}$$

A theorem due to Mattila ([14]) says that if the Hausdorff dimension of a set is greater than $\frac{d}{2}$ and if, for some Borel measure μ on E, the Mattila integral is finite, then the Lebesgue measure of the distance set is positive.

In the finite field setting, the analog of the spherical average turns out to be

$$\sigma_E(t) = \sum_{|m|^2=t} \left|\widehat{E}(m)\right|^2, \tag{1.6}$$

where here, and throughout the paper, $E(x)$ denotes the characteristic function of the set E and $\widehat{E}$ is its discrete Fourier transform, in general defined as follows.

Definition 1.5. The Fourier transform of a function $F : \mathbb{F}_q^d \to \mathbb{C}$ is given by

$$\widehat{F}(m) = q^{-d} \sum_{x \in \mathbb{F}_q^d} e^{-\frac{2\pi i m \cdot x}{q}} F(x),$$

for $m \in \mathbb{F}_q^d$, where $\mathbb{F}_q^d$ is identified with the roots of unity on the unit circle in the usual way.

If $\mathbb{F}_q = \mathbb{Z}_q$, where q is prime, then this notation can be taken literally without a need for identification. In general, the Fourier transform is defined with respect to a non-trivial principal character on $\mathbb{F}_q$, but the choice of this character has no real bearing on the calculations in this papers. We shall not assume throughout the ensuing calculations that -1 is not a square in $\mathbb{F}_q$. Whether or not -1 is a square in a given finite field has a bearing on the existence or non-existence of spheres of zero radius which play a significant role in this paper. For example, if $d = 2$, the assumption that -1 is not a square in $\mathbb{F}_q$ immediately implies that non-trivial circles of zero radius do not exist.

See, for example, [7] and [20] for the description of Fourier analysis on finite fields. We briefly summarize the relevant properties in the next section of the paper.

The finite field analog of the Mattila integral 1.5 is given by

$$\mathcal{M}_E(q) = \frac{q^{3d+1}}{(\#E)^4} \sum_{t \in \mathbb{F}_q^*} \sigma_E^2(t), \tag{1.7}$$

where $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$. Observe that in the Euclidean analog, see (1.5) above, it is irrelevant whether the lower bound of integration is 0 or 1. It will become evident later in the paper that in the finite field version the exclusion of $t = 0$ from the summation (1.7) is essential.

Our next result is a direct analog of the aforementioned theorem of Mattila ([14]).

Theorem 1.6. *Let $E \subset \mathbb{F}_q^d$, $d \geq 2$. Suppose that $\#E \geq Cq^{\frac{d}{2}}$ with C sufficiently large. Then*

$$\#\Delta(E) \gtrsim \min\left\{q, \frac{q}{\mathcal{M}_E(q)}\right\}.$$

In the Euclidean setting, a Salem set in $\mathbb{R}^d$ is a set of Hausdorff dimension s such that there exists a Borel measure μ supported on E with the property that for all ξ, such that $|\xi| > 1$,

$$|\widehat{\mu}(\xi)| \lessapprox |\xi|^{-\frac{s}{2}}.$$

One can check that the power on the right hand side cannot be increased for any s dimensional set, so the Salem property should be viewed as the optimal decay property of the Fourier transform of fractal measures.

Mattila's result can be used to easily show that if E is a Salem set of Hausdorff dimension greater than $\frac{d}{2}$, then the Lebesgue measure of the distance set is positive. Motivated by this, we introduce the following definition.

Definition 1.7. We say that $E \subset \mathbb{F}_q^d$ is a Salem set if for every non-zero element m of $\mathbb{F}_q^d$,

$$|\widehat{E}(m)| \lesssim q^{-d} \cdot \sqrt{\#E}. \tag{1.8}$$

The Salem property in the finite field setting should also be viewed as the optimal decay property for the Fourier transform. It says that $q^{-d}\sum_{x\in\mathbb{F}_q^d} e^{-\frac{2\pi i}{q}x\cdot m}E(x) \lesssim q^{-d}\cdot\sqrt{\#E}$. In other words, this is saying that the exponential sum $\sum_{x\in\mathbb{F}_q^d} e^{-\frac{2\pi i}{q}x\cdot m}E(x)$ is bounded by the square root of the number of terms we are summing over, which is the best we can, in general, expect.

In the Euclidean setting, a generalized Salem set is a set E of Hausdorff dimension s such that there exists a Borel measure μ, supported on E with the property that the spherical average

$$\int_{S^{d-1}} |\widehat{\mu}(t\omega)|^2 d\omega \lessapprox t^{-s}. \tag{1.9}$$

It is equally straightforward to show, using Mattila's result, that if E is a generalized Salem set of Hausdorff dimension greater than $\frac{d}{2}$, then the Lebesgue measure of the distance set is positive. This leads us to the following definition.

Definition 1.8. We say that $E \subset \mathbb{F}_q^d$ is a generalized Salem set if

$$\sigma_E(t) \lessapprox q^{-\frac{3d+2}{2}}(\#E)^2, \tag{1.10}$$

for $t \in \mathbb{F}_q^*$.

We could have defined generalized Salem sets differently. For example, motivated by the definition of Salem sets above, and the fact, proved in this paper, that for $t \neq 0$, $\#\{x \in \mathbb{F}_q^d : |x|^2 = t\} \approx q^{d-1}$, we could have defined a set E to be a generalized Salem set if

$$\sigma_E(t) \lesssim q^{-d-1} \cdot \#E. \tag{1.11}$$

Our reasons for choosing the definition in (1.10) will become more clear when we analyze examples in the last section of this paper. Observe that under the assumption $\#E \geq Cq^{\frac{d}{2}}$, every Salem set is a generalized Salem set. Also, as a corollary of the techniques of this paper we are going to prove the following estimate.

Lemma 1.9. *Suppose that $t \neq 0$. Then*

$$\sigma_E(t) \lesssim q^{-\frac{3d+1}{2}}(\#E)^2.$$

Unfortunately, this result is not sufficient to prove Conjecture 1.1. Our final result shows that if the set E is a Salem, or generalized Salem set, then Conjecture 1.1 indeed holds due to the decrease of $\frac{1}{2}$ in the power of q.

Theorem 1.10. *Suppose that $E \subset \mathbb{F}_q^d$ is a Salem set or a generalized Salem set of cardinality $\geq Cq^{\frac{d}{2}}$, with C sufficiently large. Then Conjecture 1.1 holds.*

In the final section of the paper, we shall see that the discrete paraboloid

$$P = \{(x, |x|^2) \in \mathbb{F}_q^{d-1} \times \mathbb{F}_q\},$$

and, if $r \neq 0$, the discrete sphere

$$S_r = \{x \in \mathbb{F}_q^d : |x|^2 = r\}$$

are Salem sets, as are their counterparts in the Euclidean setting. We shall also give examples of sets that are not Salem sets but are generalized Salem sets. We will also show there exist sets E, with $\#E$ is much greater than $q^{\frac{d}{2}}$, that are not generalized Salem sets at all. These constructions involve finding the largest possible affine sub-space contained in the sphere S_t. See Example 4.4 below. We wish to stress, however, that if $\#E$ is sufficiently close to $q^{\frac{d}{2}}$, no such examples currently exist.

It is known that in the Euclidean case, point-wise estimates on the spherical average (1.4) alone are not sufficient to prove the Falconer distance conjecture, at least in dimension two. Whether or not this may also be the case in the finite field setting is an interesting and delicate question, that we hope to address in a subsequent paper. We conclude this section by asking whether all sets such that $C_1 q^{\frac{d}{2}} \leq \#E \leq C_2 q^{\frac{d}{2}}$ are generalized Salem sets if C_1 is sufficiently large. As we indicated above, all the evidence we currently have points in this direction.

2 Finite field analog of the Fourier transform and preliminary reductions

2.1 Definitions and basic properties of the finite field Fourier transform

We start out with a quick review of basic definitions and results about the Fourier transform in finite fields. See [14] for the description of a similar method in the continuous setting. Let f be a function on $\mathbb{F}_q$. Define the kth Fourier coefficient of f by the relation

$$\widehat{f}(k) = \frac{1}{q} \sum_{j=0}^{q-1} e^{-\frac{2\pi i j k}{q}} f(j).$$

It is not difficult to show that

$$f(j) = \sum_{k \in \mathbb{F}_q} \widehat{f}(k) e^{\frac{2\pi i j k}{q}},$$

and

$$\sum_{k\in\mathbb{F}_q} |\widehat{f}(k)|^2 = \frac{1}{q}\sum_{j\in\mathbb{F}_q} |f(j)|^2. \tag{2.1}$$

Similarly, if F is a function on $\mathbb{F}_q^d$,

$$\widehat{F}(m) = \frac{1}{q^d}\sum_{x\in\mathbb{F}_q^d} e^{-\frac{2\pi i x\cdot m}{q}} F(x),$$

$$F(x) = \sum_{m\in\mathbb{F}_q^d} e^{\frac{2\pi i x\cdot m}{q}} \widehat{F}(m), \tag{2.2}$$

and

$$\sum_{m\in\mathbb{F}_q^d} |\widehat{F}(m)|^2 = \frac{1}{q^d}\sum_{x\in\mathbb{F}_q^d} |F(x)|^2. \tag{2.3}$$

We mention in passing that all the facts above can be readily verified by a direct calculation which we leave to an interested reader.

2.2 The distance set incidence function

The basic object in the study of distance sets is the incidence function

$$\begin{aligned} \nu(j) &= (\#E)^{-2}\#\{(x,y)\in E\times E : |x-y|^2 = j\} \\ &= (\#E)^{-2}\textstyle\sum_{x,y\in\mathbb{F}_q^d} E(x)E(y)S_j(x-y), \end{aligned} \tag{2.4}$$

where, as before, S_j denotes the characteristic function of the sphere $\{x : |x|^2 = j\}$. We shall give a precise argument below, but it is clear that if one has a good enough upper bound on how many times a fixed distance can occur, then one can deduce a lower bound on the total number of distances using an appropriate version of the pigeon-hole principle.

Using the Fourier inversion formula from the previous section, the latter expression equals

$$(\#E)^{-2}\sum_{x,y,m\in\mathbb{F}_q^d} e^{\frac{2\pi i(x-y)\cdot m}{q}} \widehat{S}_j(m)E(x)E(y) \tag{2.5}$$

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

By a direct calculation, $\sum_{j\in\mathbb{F}_q}\nu(j) = 1$. As we noted in the introduction, spheres of zero radius turn out to be special, so our approach is to use the Cauchy-Schwartz inequality and the fact that $(a+b)^2 \le 2a^2+2b^2$ to conclude that

$$1 = \left(\sum_{j\in\mathbb{F}_q}\nu(j)\right)^2 \le 2\nu^2(0) + 2\cdot\#\Delta(E)\cdot\sum_{j\in\mathbb{F}_q^*}\nu^2(j). \tag{2.6}$$

Lemma 2.1. *Suppose that $\#E \ge Cq^{\frac{d}{2}}$ for a sufficiently large constant C. Then there exists $0 < c < 1$ such that $2\nu^2(0) < c$.*

Lemma 2.1 follows easily from (2.5) and the following estimate on the Fourier transform of sphere.

Lemma 2.2. *Suppose that $m \neq (0, \dots, 0)$. Then*

$$|\widehat{S}_r(m)| \lesssim q^{-\frac{d+1}{2}}, \tag{2.7}$$

if $r \neq 0$, and

$$|\widehat{S}_0(m)| \lesssim q^{-\frac{d}{2}}. \tag{2.8}$$

Moreover, $\#S_0 = O(q^{d-1})$, while for $r \neq 0$, $\#S_r \approx q^{d-1}$.

The proof below also shows that the upper bound on $|\widehat{S}_0(m)|$ is only this bad if $|m|^2 = 0$ and is generally much better. In particular, Lemma 2.2 shows that if $r \neq 0$, then S_r is a Salem set. This is the key lemma of the paper and will be proved using classical bounds on Kloosterman sums originally obtained by A. Weil ([24]). This is where much of the number theoretic substance of the paper lies.

We shall need the following standard Gauss sum estimates. Let

$$G(m,k) = \sum_{x \in \mathbb{F}_q^d} e^{-\frac{2\pi i}{q}(x \cdot m - k|x|^2)}. \tag{2.9}$$

Lemma 2.3. *Suppose that $k \neq 0$. Then*

$$G(m,k) = c_k^d q^{\frac{d}{2}} e^{-\frac{2\pi i |m|^2}{4kq}},$$

where $c_k = \pm 1$, with the same choice of sign in ± 1 for all k if -1 is a square in $\mathbb{F}_q$, or else $\pm i$, with the opposite choice of signs in $\pm i$, depending on whether k is a square in $\mathbb{F}_q$ or not.

To prove the lemma, observe that

$$\begin{aligned} \sum_{x_j \in \mathbb{F}_q} e^{-\frac{2\pi i(m_j x_j - k x_j^2)}{q}} &= e^{-\frac{2\pi i m_j^2}{4kq}} \sum_{x_j \in \mathbb{F}_q} e^{\frac{2\pi i k (x_j - m_j/2k)^2}{q}} \\ &= e^{-\frac{2\pi i m_j^2}{4kq}} g(k), \end{aligned}$$

where $g(k)$ is the "standard" Gauss sum

$$g(k) = \sum_{x_j \in \mathbb{F}_q} e^{\frac{2\pi i k x_j^2}{q}}. \tag{2.10}$$

It follows that if k, k' are squares in $\mathbb{F}_q$, $g(k) = g(k')$, moreover, if -1 is a square in $\mathbb{F}_q$, then $g(k)$ is real. If -1 is not a square in $\mathbb{F}_q$, then

$$g(k) + \overline{g(k)} = \sum_{t \in \mathbb{F}_q} e^{\frac{2\pi i k t^2}{q}} + e^{-\frac{2\pi i k t^2}{q}}$$

runs over each of the elements of $\mathbb{F}_q$ exactly twice and thus equals 0. It follows that in this case $g(k)$ is purely imaginary, so $g(-k) = -g(k)$. Clearly, if -1 is not a square in $\mathbb{F}_q$, $k \neq 0$ is a square in $\mathbb{F}_q$ if and only if $-k$ is not.

The lemma now follows, as for $k \neq 0$, we have

$$G(m,k) = e^{-\frac{2\pi i |m|^2}{4kq}} g^d(k), \tag{2.11}$$

as well as the fact that

$$|g(k)| = \sqrt{q}, \tag{2.12}$$

that we are going to show next. Indeed,

$$\begin{aligned} |g(k)|^2 &= \sum_{u,v\in\mathbb{F}_q} e^{\frac{2\pi ik(u^2-v^2)}{q}} \\ &= \sum_{t\in\mathbb{F}_q} e^{\frac{2\pi ikt}{q}} n(t), \end{aligned}$$

where

$$n(t) = \#\{(u,v) \in \mathbb{F}_q \times \mathbb{F}_q : u^2 - v^2 = t\}.$$

We claim that $n(0) = 2q-1$, and $n(t) = q-1$ if $t \neq 0$. The former is obvious. To see the latter, write $u^2 - v^2 = (u-v)(u+v)$. Since $u-v$ and $u+v$ determine u and v uniquely, it suffices to count the number of solutions of the equation $u'v' = t$, $t \neq 0$. There are $q-1$ choices for u', say, and v' is completely determined. The conclusion follows.

We deduce that

$$|g(k)|^2 = q + (q-1)\sum_{t\in\mathbb{F}_q} e^{\frac{2\pi ikt}{q}} = q.$$

This completes the proof of Lemma 2.3. See, for example, [12] for a short analysis of elementary Gauss sums.

To prove Lemma 2.2, first observe that $\widehat{S}_r(m)$ should be real. With Lemma 2.3 in mind and using the notation $\delta(m) = 1$ if $m = (0,\dots,0)$ and zero otherwise, and the acronym c.c for complex conjugate, we write

$$\begin{aligned} 2\widehat{S}_r(m) &= q^{-d}\sum_{\{x\in\mathbb{F}_q^d:|x|^2=r\}} e^{-\frac{2\pi ix\cdot m}{q}} &&+ \text{ c.c} \\ &= q^{-d}\sum_{x\in\mathbb{F}_q^d} q^{-1}\sum_{j\in\mathbb{F}_q} e^{\frac{2\pi ij(|x|^2-r)}{q}} e^{-\frac{2\pi ix\cdot m}{q}} &&+ \text{ c.c} \\ &= q^{-1}\delta(m) + q^{-d-1}\sum_{j\in\mathbb{F}_q^*} e^{-\frac{2\pi ijr}{q}} \sum_{x\in\mathbb{F}_q^d} e^{\frac{2\pi ij|x|^2}{q}} e^{-\frac{2\pi ix\cdot m}{q}} &&+ \text{ c.c} \qquad (2.13) \\ &= q^{-1}\delta(m) + q^{-d-1}\sum_{j\in\mathbb{F}_q^*} e^{-\frac{2\pi ijr}{q}} G(m,j) &&+ \text{ c.c} \\ &= 2q^{-1}\delta(m) + 2q^{-\frac{d}{2}}q^{-1}\mathrm{Re}\left(c^d\sum_{j\in\mathbb{F}_q^*} e^{-\frac{2\pi i}{q}(jr+\frac{|m|^2}{4j})}\right). \end{aligned}$$

On the last step we used Lemma 2.3, and $c = \pm 1$ if -1 is a square in $\mathbb{F}_q$ and $\pm i$ otherwise.

This reduces the proof of Lemma 2.2 to the following Kloosterman sum estimate due to Andre Weil ([24]). See, for example, [8] for a nice proof.

Lemma 2.4. *For any $r, r' \in \mathbb{F}_q^*$,*

$$\left|\sum_{j\in\mathbb{F}_q^*} e^{-\frac{2\pi i}{q}(jr+j^{-1}r')}\right| \lesssim \sqrt{q}.$$

If $r \neq 0$, we immediately obtain (2.7) as well as the estimate for the cardinality of S_r, corresponding to the case $m = (0, \dots, 0)$. Indeed, if $m = (0, \dots, 0)$ and $r \neq 0$, the second term in the last line of (2.13) becomes a Gauss sum, and is negligible. If $r = 0$, we see from (2.13) that whenever $|m|^2 = 0$, $|\widehat{S_0}(m)| = O(q^{\frac{d}{2}})$. Observe that the estimate improves instantly if $|m|^2 \neq 0$ since in this case the Kloosterman sum disappears and the calculation reduces to the consideration of the Gauss sum. Also, in the case $m = (0, \dots, 0)$, $r = 0$, which corresponds to the cardinality of S_0, the second term in the last line of (2.13) is negligible, which implies that $\#S_0 \approx q^{d-1}$ for $d > 2$, while in the case $d = 2$ we can only conclude that $\#S_0 \lesssim q$. This corresponds to the fact that $\mathbb{F}_q{}^2$ will has non-trivial circles of zero radius if and only if -1 is a square in $\mathbb{F}_q$. This completes the proof of Lemma 2.2.

Using Lemma 2.1 and (2.6), we conclude that

$$\#\Delta(E) \gtrsim \frac{1}{\sum_{j \in \mathbb{F}_q^*} \nu^2(j)}. \tag{2.14}$$

The proof of Theorem 1.3 and Theorem 1.10 below mainly consists of the analysis of the quantity $\sum_{j \in \mathbb{F}_q^*} \nu^2(j)$ from various points of view using Fourier analysis and simple reductions we are in the process of making.

2.3 The Fourier transform of the incidence function

There are several ways of computing $\widehat{\nu}$. In order to emphasize the role of spheres, we choose the following approach.

Lemma 2.5. *For fixed $x \in \mathbb{F}_q^d$, let $u(j) = S_j(x)$. Then*

$$\widehat{u}(k) = q^{-1} e^{-\frac{2\pi i}{q}|x|^2 k}. \tag{2.15}$$

To prove Lemma 2.5 observe that

$$S_j(x) = q^{-1} \sum_{s \in \mathbb{F}_q} e^{-\frac{2\pi i}{q} s(|x|^2 - j)},$$

so

$$\widehat{u}(k) = q^{-2} \sum_{s \in \mathbb{F}_q} e^{-\frac{2\pi i}{q} s|x|^2} \sum_{j \in \mathbb{F}_q} e^{-\frac{2\pi i}{q} j(k-s)} = q^{-1} e^{-\frac{2\pi i}{q} k|x|^2},$$

and the proof is complete.

Combining Lemma 2.5 with (2.5) we see that

$$\begin{aligned} \widehat{\nu}(k) &= q^{2d} q^{-1} (\#E)^{-2} \textstyle\sum_{m \in \mathbb{F}_q^d} \left|\widehat{E}(m)\right|^2 q^{-d} \sum_{x \in \mathbb{F}_q^d} e^{-\frac{2\pi i}{q} x \cdot m} e^{-\frac{2\pi i}{q} k|x|^2} \\ &= q^{d-1} (\#E)^{-2} \textstyle\sum_{m \in \mathbb{F}_q^d} \left|\widehat{E}(m)\right|^2 G(m, -k). \end{aligned} \tag{2.16}$$

Applying Lemma 2.3 we see that for $k \neq 0$, we have

$$\widehat{\nu}(k) = c_k^d q^{d-1} q^{\frac{d}{2}} (\#E)^{-2} \sum_{m \in \mathbb{F}_q^d} \left|\widehat{E}(m)\right|^2 e^{\frac{2\pi i |m|^2}{4kq}}, \tag{2.17}$$

with $|c_k| = 1$.

3 Proof of Theorem 1.3, Theorem 1.4, Theorem 1.6, Lemma 1.9 and Theorem 1.10

With the preliminaries behind us, we are ready to complete the proof of Theorem 1.3. By (2.14) it suffices to estimate $\sum_{j\in\mathbb{F}_q^*}\nu^2(j)$. By (2.5), Lemma 2.2 and Plancherel (2.3),

$$\begin{aligned}\nu(j) &\lesssim q^{2d}q^{-2d}\cdot(\#E)^2\cdot\widehat{S}_j(0,\dots,0)+q^{2d}q^{-\frac{d+1}{2}}\sum_{m\neq(0,\dots,0)}\left|\widehat{E}(m)\right|^2\\ &\lesssim q^{-1}\cdot(\#E)^2+q^{\frac{d-1}{2}}\sum_{x\in\mathbb{F}_q^d}E^2(x)=q^{-1}\cdot(\#E)^2+q^{\frac{d-1}{2}}\cdot\#E.\end{aligned}$$

It follows that

$$\#\Delta(E)\gtrsim\min\left\{q,\frac{\#E}{q^{\frac{d-1}{2}}}\right\},$$

as desired, and the proof of Theorem 1.3 is complete.

In order to prove Theorem 1.4, we modify the argument above slightly. Let $j\in\mathbb{F}_q$. We have

$$\begin{aligned}\nu(j) &= \#\{(x,y)\in E\times E:|x-y|^2=j\}\\ &= \sum_{x,y}E(x)E(y)S_j(x-y)\\ &= q^{2d}\sum_m\left|\widehat{E}(m)\right|^2\widehat{S}_j(m)\\ &= (\#E)^2\widehat{S}_j(0,\dots,0)+\sum_{m\neq(0,\dots,0)}\left|\widehat{E}(m)\right|^2\widehat{S}_j(m)\\ &= I+II.\end{aligned}$$

By the same argument as in the proof of Theorem 1.3 above,

$$II\lesssim C_1\cdot\#E\cdot q^{\frac{d-1}{2}},$$

and, by the proof of Lemma 2.2,

$$I\geq C_2q^{-1}.$$

It follows that $I>II$ if

$$\#E\geq\frac{C_1}{C_2}q^{\frac{d+1}{2}},$$

and under this condition,

$$\#\{(x,y)\in E\times E:|x-y|^2=j\}>0,$$

which completes the proof of Theorem 1.4.

To prove Lemma 1.9 we use Lemma 2.2 to see that

$$\begin{aligned}\sigma_E(t) &= \sum_{|m|^2=t}\left|\widehat{E}(m)\right|^2\\ &= q^{-d}\sum_{x,y\in\mathbb{F}_q^d}E(x)E(y)\widehat{S}_t(x-y)\\ &= q^{-d}q^{-1}\sum_{x\in\mathbb{F}_q^d}E^2(x)+q^{-d}\sum_{x\neq y}E(x)E(y)\widehat{S}_t(x-y)\\ &\lesssim q^{-d-1}\cdot\#E+q^{-d}\cdot q^{-\frac{d+1}{2}}\cdot(\#E)^2,\end{aligned}$$

and the result follows.

To prove Theorem 1.6 and Theorem 1.10 we square (2.16) and (2.17) to see that

$$|\widehat{\nu}(k)|^2 = q^{3d-2}(\#E)^{-4} \sum_{m,m'} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2 e^{-\frac{2\pi i(|m|^2-|m'|^2)}{4kq}}, \tag{3.1}$$

if $k \neq 0$, and $\widehat{\nu}(0) = q^{-1} \sum_{j \in \mathbb{F}_q} \nu(j) = q^{-1}$.

Now, using (3.1), we see that

$$\begin{aligned} \sum_{k \in \mathbb{F}_q} |\widehat{\nu}(k)|^2 &= q^{-2} + \frac{q^{3d-1}}{(\#E)^4} \sum_{|m|^2=|m'|^2} |\widehat{E}(m)|^2 |\widehat{E}(m')|^2 \\ &= q^{-2} + \frac{q^{3d-1}}{(\#E)^4} \sum_{t \in \mathbb{F}_q^*} \sigma_E^2(t) + \frac{q^{3d-1}}{(\#E)^4} \sigma_E^2(0). \end{aligned}$$

In view of (2.14), we are interested in computing

$$\sum_{j \in \mathbb{F}_q^*} \nu^2(j) = \sum_{j \in \mathbb{F}_q} \nu^2(j) - \nu^2(0)$$

$$= q^{-1} + q^{-1} \frac{q^{3d+1}}{(\#E)^4} \sum_{t \in \mathbb{F}_q^*} \sigma_E^2(t) + q^{-1} \frac{q^{3d+1}}{(\#E)^4} \sigma_E^2(0) - \nu^2(0).$$

Now,

$$\sigma_E(0) = \sum |\widehat{E}(m)|^2 S_0(m) = q^{-d} \sum_{x,y \in \mathbb{F}_q^d} E(x)E(y)\widehat{S}_0(x-y). \tag{3.2}$$

Using (2.13) and (3.2) we see that

$$\sigma_E^2(0) = q^{-3d}(\#E)^4 \nu^2(0) + O(q^{-3d-1}(\#E)^4).$$

It follows that

$$q^{-1} \frac{q^{3d+1}}{(\#E)^4} \sigma_E^2(0) - \nu^2(0) = O(q^{-1}).$$

We conclude, using (2.5) that

$$\#\Delta(E) \gtrsim \min\left\{q, \frac{q}{\mathcal{M}_E(q)}\right\},$$

as desired. This completes the proof of Theorem 1.6.

In order to prove Theorem 1.10, observe that the definition of a Salem set combined with Lemma implies that for $t \neq 0$,

$$\sigma_E(t) \leq \#S_t \cdot q^{-2d} \cdot \#E \lesssim q^{-d-1} \cdot \#E. \tag{3.3}$$

It follows that

$$\begin{aligned} \mathcal{M}_E(q) &\lesssim \frac{q^{2d}}{(\#E)^3} \sum_{t \in \mathbb{F}_q^*} \sum_{|m|^2=t} |\widehat{E}(m)|^2 \\ &\lesssim \frac{q^{2d}}{(\#E)^3} \sum_{m \in \mathbb{F}_q^d} |\widehat{E}(m)|^2 \\ &= \frac{q^d}{(\#E)^3} \sum_{x \in \mathbb{F}_q^d} E^2(x) \\ &= \frac{q^d}{(\#E)^2} \\ &\lesssim 1, \end{aligned}$$

if $\#E \gtrsim q^{\frac{d}{2}}$. In view of (3.3) the same conclusion holds if E is a generalized Salem set. This completes the proof of Theorem 1.10.

4 Examples of Salem and non-Salem sets, and non generalized Salem sets

We have already seen that the sphere of non-zero radius is a Salem set. We now show that the paraboloid is a Salem set as well.

Example 4.1. Let $E = \{(x, |x|^2) : x \in \mathbb{F}_q^{d-1}\}$. Then E is a Salem set.

To prove this, observe that $\#E = q^{d-1}$. Furthermore,

$$\widehat{E}(m,t) = q^{-d} \sum_{x \in \mathbb{F}_q^{d-1}} e^{-\frac{2\pi i(m\cdot x + t|x|^2)}{q}}.$$

Using (2.11) and (2.12) we see that

$$|\widehat{E}(m,t)| \lesssim q^{-d} q^{\frac{d-1}{2}},$$

and the claim is proved.

Our second example shows that not all sets are Salem sets.

Example 4.2. Let $d = 2$ and

$$E = \{(k,k) : k \in \mathbb{F}_q\}.$$

Then E is not a Salem set but is a generalized Salem set.

To prove this observe that

$$\widehat{E}(m) = q^{-2} \sum_{k \in \mathbb{F}_q} e^{-\frac{2\pi i(m_1+m_2)k}{q}}$$

$$= q^{-1} E'(m),$$

where

$$E' = \{(t,-t) : t \in \mathbb{F}_q\}.$$

This shows that E' is not a Salem set. On the other hand,

$$\sigma_E(t) = \sum_{|m|^2 = t} q^{-2} E'(m) = O(q^{-2})$$

if $t \neq 0$. Since $\#E = q$, this implies that E is a generalized Salem set.

Next, we give an example of a generalized Salem set in the sense of Definition 1.8 that does not satisfy (1.11).

Example 4.3. Let $v \in \mathbb{F}_q^4$ such that $|v|^2 = 0$ and such that $z_1v_1 + z_2v_2 + \cdots + z_dv_d = 0$ for some $z \in S_1 = \{x \in \mathbb{F}_q^4 : |x|^2 = 1\}$. (The existence of such a v can be verified by a direct computation. See, for example, [22].) Let E denote the hyper-pane $\{x \in \mathbb{F}_q : x \cdot v = 0\}$. Then E is a generalized Salem set in the sense of Definition 1.8, but it would not be a generalized Salem set had we gone with the definition given by (1.11).

To see this observe that the line $\{z+tv : t \in \mathbb{F}_q\}$ is contained in S_1 since $(z+tv)\cdot(z+tv) = |z|^2 = 1$. We next observe that

$$\widehat{E}(m) = q^{-1}E'(m),$$

where $E' = \{z + tv : t \in \mathbb{F}_q\}$. Now,

$$\sigma_E(1) = q^{-2} \sum_{|m|^2=1} E'(m) = q^{-1}.$$

Since $q^{-d-1} \cdot \#E = q^{-5} \cdot q^3 = q^{-2}$. This proves our claim.

In conclusion, we give an example of sets that are not generalized Salem.

Example 4.4. Suppose that there exists an affine k-plane E' in $\mathbb{F}_q^d$, with $k > \frac{d}{2} - 1$, contained in the sphere S_t for some $t \neq 0$. If the answer is yes, it follows that the set $E = \{x \in \mathbb{F}_q^d : x \cdot y = 0, \ \forall \ y \in E'\}$ is not a generalized Salem set. Indeed, we would have

$$\sigma_E(t) = q^{-2k} \sum_{|m|^2=t} E'(m) = q^{-k}.$$

Now, $q^{-d-1} \cdot \#E \cdot \#E \cdot q^{-\frac{d}{2}} = q^{\frac{d}{2}-1}q^{-2k}$. If $k > \frac{d}{2} - 1$, $\frac{d}{2} - 1 - 2k < -k$, so E is not a generalized Salem set.

If -1 is a square in $\mathbb{F}_q$, and d is odd, such a k plane exists. Indeed, if -1 is a square in $\mathbb{F}_q$, then there exists a one-dimensional linear subspace L_0 in $\mathbb{F}_q^2$, such that for any $(u, v) \in L_0$, $u^2 + v^2 = 0$. Fix some such $(u, v) \neq (0, 0)$. For $j = 1, ..., (d-1)/2$, let L_j be the one-dimensional subspace, spanned by the vectors $ue_{2j} + ve_{2j+1}$, where e_j is the unit vector in the direction of the coordinate x_j in $\mathbb{F}_q^d$. Take the direct sum

$$\Pi = L_1 + ... + L_{(d-1)/2},$$

and let $E = (1, 0, \ldots, 0) + \Pi$. Then E is a $\frac{d-1}{2}$-dimensional affine plane contained in the unit sphere in $\mathbb{F}_q^d$.

We remark in passing that with a bit more work, e.g. elaborating on the construction following Question 1.2, one can construct, for every $\epsilon > 0$ a set of cardinality $\approx q^{\frac{d}{2}+\epsilon}$ which is not a generalized Salem set. Details are left to the interested reader.

References

[1] J. Pach, and P. Agarwal, *Combinatorial geometry,* Wiley-Interscience Series in Discrete Mathematics and Optimization. A Wiley-Interscience Publication. John Wiley and Sons, Inc., New York (1995).

[2] J. Bourgain, *Hausdorff dimension and distance sets,* Israel. J. Math. **87** (1994), 193–201.

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

[4] B. Erdoğan, *A bilinear Fourier extension theorem and applications to the distance set problem,* Internat. Math. Res. Notices **23** (2005), 1411–1425.

[5] P. Erdös *On sets of distances of n points,* Amer. Math. Monthly. **53** (1946), 248–250.

[6] K. J. Falconer, *On the Hausdorff dimensions of distance sets,* Mathematika **32** (1985), 206–212.

[7] B. J. Green, *Restriction and Kakeya phonomena,* Lecture notes (2003).

[8] H. Iwaniec, and E. Kowalski, *Analytc Number Theory,* Colloquium Publications **53** (2004).

[9] A. Iosevich, and M. Rudnev, *On distance measures for well-distributed sets*, preprint (2006).

[10] N. Katz, *Gauss sums, Kloosterman sums, and monodromy groups,* Ann. Math. Studies **1**16, Princeton (1988).

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

[12] E. Landau, *Vorlesungen über Zahlentheorie,* Chelsea Publishing Co., New York (1969).

[13] J. Matousek, *Lectures on Discrete Geometry,* Graduate Texts in Mathematics, Springer **202** (2002).

[14] P. Mattila, *Spherical averages of Fourier transforms of measures with finite energy: dimensions of intersections and distance sets* Mathematika, **34** (1987), 207–228.

[15] P. Mattila, and P. Sjölin, *Regularity of distance measures and sets,* Math. Nachr. **204** (1999), 157–162.

[16] L. Moser, *On the different distances determined by n points,* Amer. Math. Monthly **59** (1952), 85–91.

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

[18] H. Niederreiter, *The distribution of values of Kloosterman sums,* Arch. Math. **56** (1991), 270–277.

[19] Y. Peres, and W. Schlag, *Smoothness of projections, Bernoulli convolutions, and the dimension of exceptions,* Duke Math. J. **102** (2000), 193–251.

[20] E. Stein, and R. Shakarchi, *Fourier analysis,* Princeton Lectures in Analysis, (2003).

[21] T. Tao, *Finite field analogues of Erdös, Falconer, and Furstenberg problems,* preprint.

[22] T. Tao, *A new bound for finite field Besicovitch sets in four dimensions,* Pacific J. Math. **222**, no 2 (2005), 337–363.

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

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