Hamming Distances in Vector Spaces over Finite Fields

Esen Aksoy Yazici

October 15, 2019

Abstract

Let $\mathbb{F}_q$ be the finite field of order $q$ and $E \subset \mathbb{F}_q^d$, where $4|d$. Using Fourier analytic techniques, we prove that if $|E| > \frac{q^{d-1}}{d} \binom{d}{d/2} \binom{d/2}{d/4}$, then the points of $E$ determine a Hamming distance $r$ for every even $r$.

1 Introduction

Let $\mathbb{F}_q$ be the finite field with order $q$, where $q = p^l$ and $p$ is an odd prime. In the vector space $\mathbb{F}_q^d$, we can consider the following distance map

$$\lambda : (x, y) \mapsto \|x - y\| = (x_1 - y_1)^2 + \ldots + (x_d - y_d)^2.$$  \hspace{1cm} (1.1)

For $E \subset \mathbb{F}_q^d$, let $\Delta(E)$ denote the set of distances determined by the points of $E$ that is,

$$\Delta(E) := \{\|x - y\| : x, y \in E\}.$$

The Erdős-Falconer distance problem in $\mathbb{F}_q^d$ asks for a threshold on the size $E \subset \mathbb{F}_q^d$ so that $\Delta(E)$ contains a positive proportion of $\mathbb{F}_q$. In $\mathbb{F}_q$, Iosevich and Rudnev proved that for $E \subset \mathbb{F}_q^d$ if $|E| > cq^{d+1}$ for a sufficiently large constant $c$, then $\Delta(E) = \mathbb{F}_q$.

Erdős-Falconer distance problem in modules $\mathbb{Z}_q^d$ over the cyclic rings $\mathbb{Z}_q$ was studied by Covert, Iosevich and Pakianathan in $[5]$. More precisely, it is proven that for $E \subset \mathbb{Z}_q^d$ where $q = p^l$, if $|E| \gg l(l+1)q^{\frac{(2l+1)d}{2l+2}}$, then $\Delta(E)$ contains all unit elements of $\mathbb{Z}_q$.

For more literature on the distance introduced in (1.1) and related geometric configurations, we refer to $[1-4, 6, 7, 9]$ and the references therein.

Here, in this paper, we tackle a similar problem related to coding theory. Instead of the distance given in (1.1), we consider the Hamming distance in $\mathbb{F}_q^d$, a key notion in coding theory, and ask similar geometric configurations in $\mathbb{F}_q^d$. We note that the approach we use to prove the main theorem of this paper is analogous to the one employed in $[5]$ and $[8]$. Let us first recall the necessary notion.
For two vectors \( x = (x_1, \ldots, x_d), y = (y_1, \ldots, y_d) \in \mathbb{F}_q^d \), the Hamming distance between \( x \) and \( y \) is defined as

\[
|x - y| = \sum_{i=1}^{d} d(x_i, y_i)
\]

where

\[
d(x_i, y_i) = 1 - \delta_{x_i, y_i} = \begin{cases} 
0 & \text{if } x_i = y_i, \\
1 & \text{if } x_i \neq y_i.
\end{cases}
\]

In other words, the Hamming distance \( |x - y| \) between \( x \) and \( y \) is the number of coordinates in which \( x \) and \( y \) differ. In particular, \( |x| \) is the number of nonzero coordinates of \( x \). We will denote the Hamming weight of \( x \) as \( \text{wt}(x) \).

The question we will be dealing with in this note is that for subsets \( E \subseteq \mathbb{F}_q^d \), which can be seen as a code over \( \mathbb{F}_q \), how large does the size of \( E \) need to be to guarantee that \( E \) contains the desired set of Hamming distances.

1.1 Main Result

**Theorem 1.1.** Let \( E \subseteq \mathbb{F}_q^d \) where \( 4 \mid d \). If \( |E| > q^{d-1} \left( \frac{d}{d/2} \right)^{d/4} \), then the points of \( E \) determine a Hamming distance \( r \) for every even \( r \).

1.2 Fourier Analysis in \( \mathbb{F}_q^d \)

Let \( f : \mathbb{F}_q^d \to \mathbb{C} \). The Fourier transform of \( f \) is defined as

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

where \( \chi(z) = e^{2\pi \text{Tr}(z)/q} \), \( q = p^l \), \( p \) prime, and \( \text{Tr} : \mathbb{F}_q \to \mathbb{F}_p \) is the Galois trace.

We recall the following properties of Fourier transform.

\[
q^{-d} \sum_{x \in \mathbb{F}_q^d} \chi(x \cdot m) = \begin{cases} 
1, & \text{if } m = 0 \\
0, & \text{otherwise}
\end{cases} \quad \text{(Orthogonality)}
\]

\[
f(x) = \sum_{m \in \mathbb{F}_q^d} \chi(x \cdot m) \hat{f}(m) \quad \text{(Inversion)}
\]

\[
\sum_{m \in \mathbb{F}_q^d} |\hat{f}(m)|^2 = q^{-d} \sum_{x \in \mathbb{F}_q^d} |f(x)|^2. \quad \text{(Plancherel)}
\]
2 Proof of Main Result

For the proof of Theorem 1.1, we make use of the following lemmas:

Lemma 2.1. Let $S_r(u) = \{ v \in \mathbb{F}_q^d : |u - v| = r \}$ be the sphere of radius $r$ centered at $u \in \mathbb{F}_q^d$. Then

$$|S_r(u)| = (q - 1)^r \binom{d}{r}.$$ 

Proof. If $v \in S_r(u)$, then $u$ and $v$ differ in $r$ coordinates. Note that we have $\binom{d}{r}$ ways of choosing those $r$ coordinates, and for each of these $r$ coordinates of $v$ we have $q - 1$ choices.

Lemma 2.2. Let $S_r := S_r(0) = \{ v \in \mathbb{F}_q^d : |v| = r \}$ denote the sphere of radius $r$ centered at $0 \in \mathbb{F}_q^d$, where $4 \nmid d$, and identify $S_r$ with its indicator function. Then

$$\sup_{0 \neq m \in \mathbb{F}_q^d} |\hat{S}_r(m)| = q^{-d} \sup_{0 \neq m \in \mathbb{F}_q^d} |K_r(wt(m))| \leq \begin{cases} q^{-d}(\frac{d}{d/2})(\frac{d/2}{d/4}) & \text{if } wt(m) \text{ is even} \\ q^{-d}(q - 1)^{r-1}(\frac{d}{d/2})(\frac{d}{d/4}) & \text{if } wt(m) \text{ is odd and } r \text{ is even} \end{cases}$$

Proof.

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

$$= q^{-d} \sum_{x_1, \ldots, x_r \in \mathbb{F}_q^d} \chi(-x_1m_{i_1} - \cdots - x_r m_{i_r})$$

$$= q^{-d} \sum_{x_1, \ldots, x_r \in \mathbb{F}_q^d \atop i_j \in \{1, \ldots, d\} \atop i_j \neq i_k} e^{-\frac{2\pi i}{q}(x_1m_{i_1} + \cdots + x_r m_{i_r})}$$

$$= q^{-d} \sum_{|I^k| = r \atop I^k = \{k_1, \ldots, k_r\}} \prod_{i=1}^r \sum_{x_i \in \mathbb{F}_q^d} e^{-\frac{2\pi i}{q}(x_i m_{k_i})}$$

$$= q^{-d} \sum_{\{k_1, \ldots, k_r\} \subset \{1, \ldots, d\} \atop k_i < k_j \text{ for } i < j} \left( \sum_{x_1 \in \mathbb{F}_q^d} e^{-\frac{2\pi i}{q}(x_1 m_{k_1})} \cdots \sum_{x_r \in \mathbb{F}_q^d} e^{-\frac{2\pi i}{q}(x_r m_{k_r})} \right)$$

$\square$
First note that
\[
\sum_{x_i \in \mathbb{F}_q^*} e^{-\frac{2\pi i}{q} (x_i m_{k_i})} = \begin{cases} 
q - 1 & \text{if } m_{k_i} = 0 \\
-1 & \text{if } m_{k_i} \neq 0.
\end{cases}
\]

Now let \( wt(m) = t \), \( m = (m_1, \ldots, m_t, \ldots, m_d) \), where \( m_i \neq 0 \) for \( i = 1, \ldots, t \) and \( m_i = 0 \) for \( i = t + 1, \ldots, d \). For a fixed \( I^k = (k_1, \ldots, k_r) \), let
\[
S_{I^k} = \left( \sum_{x_1 \in \mathbb{F}_q^*} e^{-\frac{2\pi i}{q} (x_1 m_{k_1})} \cdots \sum_{x_r \in \mathbb{F}_q^*} e^{-\frac{2\pi i}{q} (x_r m_{k_r})} \right).
\]
Here if \( i \) coordinates of \((m_{k_1}, \ldots, m_t, \ldots, m_{k_r})\) are nonzero, then we get
\[
S_{I^k} = (-1)^i(q - 1)^{r-i},
\]
and we have \( \binom{d}{t} \binom{d-t}{r-i} \) many such \((m_{k_1}, \ldots, m_t, \ldots, m_{k_r})\). Summing over all possible \( i \)'s, \( i = 0, \ldots, t \), we get
\[
\hat{S}_r(m) = q^{-d} \sum_{i=0}^{r} \binom{t}{i} \binom{d-t}{r-i} (-1)^i (q - 1)^{r-i} \tag{2.1}
\]
\[
= q^{-d} K_r(t) = q^{-d} K_r(wt(m))
\]
where \( K_r(\cdot) \) denotes the Krawtchouk polynomial.

We will make use of the following two lemmas from [10].

**Lemma 2.3.** [10, Lemma 1] For \( d \) and \( i \) even
\[
|K_{k}(i)| \leq |K_{d/2}(i)|
\]

**Lemma 2.4.** [10, Lemma 2] For \( k \) integer, \( d \) and \( i \) even
\[
|K_{k}(i)| \leq \frac{\binom{d}{d/2} \binom{d/2}{i/2}}{\binom{d}{k}}
\]
Now using Lemmas 2.3 and 2.4, we immediately obtain that if \( wt(m) \) is even, then
\[
\sup |\hat{S}_r(m)| \leq q^{-d} \left( \frac{d}{d/2} \right) \left( \frac{d/2}{d/4} \right)
\]
On the other hand, if \( wt(m) = i \) is odd, then using the symmetry relation of Krawtchouk polynomials, now assuming that \( r \) is even , we obtain
\[ |\tilde{S}_r(m)| = q^{-d}K_r(wt(m)) \]
\[ = q^{-d}K_r(i) \]
\[ = q^{-d}(q-1)^r \frac{\binom{d}{i}}{(q-1)^i} K_i(r) \]
\[ \leq q^{-d}(q-1)^{r-i} \frac{\binom{d}{i}}{(d/2)^i} \binom{d/2}{d/4} \]
\[ \leq q^{-d}(q-1)^{r-i} \frac{d}{d} \frac{d/2}{d/4} \]

Proof of Theorem 1.1. Let \(0 < r < d\) be even. Let \(\lambda_r = |\{(x,y) \in E \times E : |x-y| = r\}|\). Then

\[ \lambda_r = \sum_{x,y \in \mathbb{F}_q^d} E(x)E(y)S_r(x-y) \]
\[ = \sum_{x,y,m \in \mathbb{F}_q^d} E(x)E(y)\tilde{S}_r(m)\chi(m \cdot (x-y)) \]
\[ = q^{2d} \sum_m |\hat{E}(m)|^2\tilde{S}_r(m) \]
\[ = q^{2d}|\hat{E}(0)|^2\tilde{S}_r(0) + q^{2d} \sum_{m \neq 0} |\hat{E}(m)|^2\tilde{S}_r(m) \]
\[ = q^{-d}|E|^2S_r + q^{2d} \sum_{m \neq 0} |\hat{E}(m)|^2\tilde{S}_r(m) \]
\[ = q^{-d}|E|^2(q-1)^r \binom{d}{r} + q^{2d} \sum_{m \neq 0 \text{ wt}(m) \text{ is even}} |\hat{E}(m)|^2\tilde{S}_r(m) + q^{2d} \sum_{m \neq 0 \text{ wt}(m) \text{ is odd}} |\hat{E}(m)|^2\tilde{S}_r(m) \]
\[ = q^{-d}|E|^2(q-1)^r \binom{d}{r} + I + II \]  \tag{2.2}

where

\[ I = q^{2d} \sum_{m \neq 0 \text{ wt}(m) \text{ is even}} |\hat{E}(m)|^2\tilde{S}_r(m) \]

and

\[ II = q^{2d} \sum_{m \neq 0 \text{ wt}(m) \text{ is odd}} |\hat{E}(m)|^2\tilde{S}_r(m) \]
We will first estimate $|I|$. By Lemma 2.2 and Plancherel identity, it follows that

$$|I| \leq q^{2d}q^{-d} \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)} \sum_{m \neq 0 \atop \text{wt}(m) \text{ is even}} |\hat{E}(m)|^2$$

$$\leq q^{d} \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)} \sum_{m \neq 0} |\hat{E}(m)|^2$$

$$\leq q^{d} \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)} q^{-d} |E|$$

$$= \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)} |E|$$

Now we will estimate $|II|$. Again using Lemma 2.2 and Plancherel identity, we obtain that

$$|II| \leq q^{2d}q^{-d}(q - 1)^{r-1} \left( \frac{d}{d} \right)^{\left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)}} \sum_{m \neq 0 \atop \text{wt}(m) \text{ is odd}} |\hat{E}(m)|^2$$

$$\leq q^{d}(q - 1)^{r-1} \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)} \sum_{m \neq 0} |\hat{E}(m)|^2$$

$$\leq q^{d+r-1} \left( \frac{d}{d} \right)^{\left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)}} q^{-d} |E|$$

$$= q^{r-1} \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)} |E|$$

Clearly, $|I| \leq |II|$

It follows from (2.2) that, if $q^{-d}|E|^2(q - 1)^{r} \left( \frac{d}{d} \right)^{\left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)}} |E|$, that is if

$$|E| > q^{d-1} \left( \frac{d}{d/2} \right)^{\left( \frac{d}{d/4} \right)}$$

then \( \lambda_r > 0 \).

\[ \square \]

References

[1] M. Bennett, D. Hart, A. Iosevich, J. Pakianathan, and M. Rudnev, Group actions and geometric combinatorics in \( \mathbb{F}_q^d \), Forum Math. 29 (2017), no. 1, 91110.

[2] M. Bennett, A, Iosevich and J. Pakianathan, Three-point configurations determined by subsets of \( \mathbb{F}_q^2 \) via the Elekes-Sharir paradigm, Combinatorica 34 (2014), no. 6, 689-706.
[3] J. Chapman, M. B. Erdogan, D. Hart, A. Iosevich and D. Koh, *Pinned distance sets, k-simplices, Wolff’s exponent in finite fields and sum-product estimates*, Mathematische Zeitschrift, Math. Z. 271(2012) no. 1-2, 63-93. 1

[4] D. Covert, D. Hart, A. Iosevich, S. Senger, I. Uriarte-Tuero, *A Furstenberg-Katznelson-Weiss type theorem on (d + 1)-point configurations in sets of positive density in finite field geometries*. Discrete Math. 311 (2011), no. 6, 423-430. 1

[5] D. Covert, A. Iosevich, J. Pakianathan, *Geometric configurations in the ring of integers modulo p*, Indiana Univ. Math. J. 61 (2012), no. 5, 1949-1969. 1

[6] D. Hart, A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint*, Radon transforms, geometry, and wavelets, 129-135, Contemp. Math., 464, Amer. Math. Soc., Providence, RI, 2008. 1

[7] D. Hart, A. Iosevich, D. Koh and M. Rudnev, *Averages over hyperplanes, sum-product theory in finite fields, and the Erdős-Falconer distance conjecture*, Transaction of the AMS, 363 (2011) 3255-3275. 1

[8] A. Iosevich and M. Rudnev, *Erdős distance problem in vector spaces over finite fields*, Trans. Amer. Math. Soc. 359 (2007) no. 12, 6127-6142. 1

[9] A. Iosevich, M. Rudnev, and Y. Zhai, *Areas of triangles and Beck’s theorem in planes over finite fields*, Combinatorica 35 (2015), no. 3, 295308. 1

[10] I. Krasikov, S. Litsyn, *On spectra of BCH codes*. IEEE Trans. Inform. Theory 41 (1995), no. 3, 786790. 4