ON THE SET OF DISTANCES BETWEEN TWO SETS OVER FINITE FIELDS

IGOR E. SHPARLINSKI

Received 13 March 2006; Revised 12 May 2006; Accepted 9 July 2006

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

1. Introduction

For a ring $\mathcal{R}$ and two finite sets $\mathcal{A},\mathcal{B} \subseteq \mathcal{R}^n$, we denote by $\Gamma(\mathcal{R}^n,\mathcal{A},\mathcal{B})$ the number of distinct distances between all pairs of points $(\mathbf{x},\mathbf{y}) \in \mathcal{A} \times \mathcal{B}$, that is,

$$\Gamma(\mathcal{R}^n,\mathcal{A},\mathcal{B}) = \left|\{d(\mathbf{x},\mathbf{y}) \mid (\mathbf{x},\mathbf{y}) \in \mathcal{A} \times \mathcal{B}\}\right|, \tag{1.1}$$

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

$$d(\mathbf{x},\mathbf{y}) = \sum_{j=1}^{n} (x_j - y_j)^2. \tag{1.2}$$

In the case $\mathcal{A} = \mathcal{B}$ the problem of estimating $\Gamma(\mathcal{R}^n,\mathcal{A},\mathcal{A})$ is well known. In particular, the *Erdös distance conjecture* asserts that over the real numbers, that is, for $\mathcal{R} = \mathbb{R}$, the bound

$$\Gamma(\mathbb{R}^n,\mathcal{A},\mathcal{A}) \geq c(\varepsilon)|\mathcal{A}|^{2/n-\varepsilon} \tag{1.3}$$

holds for an arbitrary $\varepsilon > 0$ and any finite set $\mathcal{A} \in \mathbb{R}^n$, where $c(\varepsilon) > 0$ depends only on ε. Despite that there are some very interesting lower bounds on $\Gamma(\mathbb{R}^n,\mathcal{A},\mathcal{A})$, this conjecture is still widely open in any dimension including $n = 2$. For some recent achievements and generalisations, see [1–6] and references therein.

Iosevich and Rudnev [4] have recently considered this problem for sets over finite fields (again for $\mathcal{A} = \mathcal{B}$) and obtained several very interesting results.

Hindawi Publishing Corporation
International Journal of Mathematics and Mathematical Sciences
Volume 2006, Article ID 59482, Pages 1–5
DOI 10.1155/IJMMS/2006/59482

The case of arbitrary sets $\mathcal{A},\mathcal{B} \in \mathbb{F}_q^n$ has recently been studied in [8], where the lower bound

$$\Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) > q - \frac{q^{n+2}}{|\mathcal{A}||\mathcal{B}|} \tag{1.4}$$

is given (which in some special case is new even for $\mathcal{A} = \mathcal{B}$). In particular, it is nontrivial for $|\mathcal{A}||\mathcal{B}| > q^{n+1}$. The method of [8] rests on a new bound of exponential sums over the set of distances. Here we use this bound in a slightly different way to derive an improvement of (1.4), which is nontrivial for $|\mathcal{A}||\mathcal{B}| > q^n$.

In fact, one can easily adjust the method of [4] to the case of distinct sets $\mathcal{A}$ and $\mathcal{B}$, or in fact derive a lower bound on $\Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})$ from already existing results of [4]. Such bounds are usually stronger than the bound of this work. However in some extremal cases our approach leads to a bound of the same order of magnitude which has completely explicit (and perhaps better than those one can extract from [4]) constants. For example, one can derive from [4] that if $|\mathcal{A}||\mathcal{B}| > Cq^{n+1}$, then $\Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) = q$, provided that C is sufficiently large.

Furthermore, as in [8], given n polynomials $f_j(X,Y) \in \mathbb{F}_q[X,Y]$, $j = 1,\dots,n$, we define the *generalised distance*

$$d_{\mathbf{f}}(\mathbf{x},\mathbf{y}) = \sum_{j=1}^{n} f_j(x_j,y_j), \tag{1.5}$$

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

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

$$\Gamma_{\mathbf{f}}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) = \left|\{d_{\mathbf{f}}(\mathbf{x},\mathbf{y}) \mid \mathbf{x}\in\mathcal{A},\ \mathbf{y}\in\mathcal{B}\}\right|. \tag{1.6}$$

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

$$\Gamma_{\mathbf{f}_0}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) = \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}). \tag{1.7}$$

In particular, under some conditions on $\mathbf{f}$, the bound

$$\Gamma_{\mathbf{f}}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) = q + O\left(\frac{q^{3n/2+2}}{|\mathcal{A}||\mathcal{B}|}\right) \tag{1.8}$$

has been given in [8]. Here we show that the power of q in the error term can be lowered to $q^{3n/2+1}$.

2. Euclidean distances

We start with the case of Euclidean distances and improve the bound (1.4).

Theorem 2.1. *For arbitrary sets* $\mathcal{A},\mathcal{B} \subseteq \mathbb{F}_q^n$,

$$\Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) > \frac{|\mathcal{A}||\mathcal{B}|q}{q^{n+1}+|\mathcal{A}||\mathcal{B}|}. \tag{2.1}$$

Proof. Let χ be a nontrivial additive character of $\mathbb{F}_q$ (see [7] for basis properties of additive characters). In particular, we recall the identity

$$\sum_{s\in\mathbb{F}_q}\chi(st)=\begin{cases}0 & \text{if } t\in\mathbb{F}_q^*,\\ q & \text{if } t=0.\end{cases} \tag{2.2}$$

As in [8], we consider character sums

$$S(a,\mathcal{A},\mathcal{B})=\sum_{\mathbf{x}\in\mathcal{A}}\sum_{\mathbf{y}\in\mathcal{B}}\chi\big(ad(\mathbf{x},\mathbf{y})\big),\quad a\in\mathbb{F}_q, \tag{2.3}$$

where as before $d(\mathbf{x},\mathbf{y})$ is given by (1.2).

Our principal tool is the upper bound

$$\big|S(a,\mathcal{A},\mathcal{B})\big|\le\sqrt{|\mathcal{A}||\mathcal{B}|q^n}, \tag{2.4}$$

which is established in [8] for any $a\in\mathbb{F}_q^*$.

For $\lambda\in\mathbb{F}_q$, we denote by $N(\lambda)$ the number of representations $\lambda=d(\mathbf{x},\mathbf{y})$ with $(\mathbf{x},\mathbf{y})\in\mathcal{A}\times\mathcal{B}$.

Then by (2.2) we have

$$N(\lambda)=\frac{1}{q}\sum_{\mathbf{x}\in\mathcal{A}}\sum_{\mathbf{y}\in\mathcal{B}}\frac{1}{q}\sum_{a\in\mathbb{F}_q}\chi\big(a\big(d(\mathbf{x},\mathbf{y})-\lambda\big)\big)=\frac{1}{q}\sum_{a\in\mathbb{F}_q}\chi(-a\lambda)S(a,\mathcal{A},\mathcal{B}). \tag{2.5}$$

Hence,

$$\begin{aligned}\sum_{\lambda\in\mathbb{F}_q}N(\lambda)^2&=\frac{1}{q^2}\sum_{\lambda\in\mathbb{F}_q}\sum_{a,b\in\mathbb{F}_q}\chi\big((b-a)\lambda\big)S(a,\mathcal{A},\mathcal{B})\overline{S(b,\mathcal{A},\mathcal{B})}\\&=\frac{1}{q^2}\sum_{a,b\in\mathbb{F}_q}S(a,\mathcal{A},\mathcal{B})\overline{S(b,\mathcal{A},\mathcal{B})}\sum_{\lambda\in\mathbb{F}_q}\chi\big((b-a)\lambda\big)\\&=\frac{1}{q}\sum_{a\in\mathbb{F}_q}\big|S(a,\mathcal{A},\mathcal{B})\big|^2,\end{aligned} \tag{2.6}$$

since by (2.2) the sum over λ vanishes unless $a=b$.

We now use the bound (2.4) for $a\in\mathbb{F}_q^*$ and the trivial bound $|S(a,\mathcal{A},\mathcal{B})|\le|\mathcal{A}||\mathcal{B}|$ for $a=0$, getting

$$\sum_{\lambda\in\mathbb{F}_q}N(\lambda)^2<|\mathcal{A}||\mathcal{B}|q^n+|\mathcal{A}|^2|\mathcal{B}|^2q^{-1}. \tag{2.7}$$

Clearly

$$\sum_{\lambda\in\mathbb{F}_q}N(\lambda)=|\mathcal{A}||\mathcal{B}|. \tag{2.8}$$

Now by the Cauchy inequality we derive

$$\begin{aligned}(|\mathcal{A}||\mathcal{B}|)^2 = \left(\sum_{\lambda\in\mathbb{F}_q} N(\lambda)\right)^2 &\le \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) \sum_{\lambda\in\mathbb{F}_q} N(\lambda)^2 \\ &< \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})\left(|\mathcal{A}||\mathcal{B}|q^n + |\mathcal{A}|^2|\mathcal{B}|^2,q^{-1}\right),\end{aligned} \tag{2.9}$$

which implies the desired result. □

3. Generalised distances

We now use similar arguments to improve the bound (1.8).

Theorem 3.1. *Let* $\mathbf{f} = (f_1,\ldots,f_n)$, *where each of the polynomials* $f_j(X,Y) \in \mathbb{F}_q[X,Y]$, $j = 1,\ldots,n$, *is of degree at most k and is not of the form* $f_j(X,Y) = g_j(X) + h_j(Y)$ *with* $g_j(X) \in \mathbb{F}_q[X]$, $h_j(Y) \in \mathbb{F}_q[Y]$. *Then, for arbitrary sets* $\mathcal{A},\mathcal{B} \subseteq \mathbb{F}_q^n$,

$$\Gamma_{\mathbf{f}}(\mathbb{F}_q^n,\mathcal{A},\mathcal{B}) = q + O\left(\frac{q^{3n/2+1}}{|\mathcal{A}||\mathcal{B}|}\right). \tag{3.1}$$

Proof. Here, instead of the bound (2.4), we use the bound

$$|S_{\mathbf{f}}(a,\mathcal{A},\mathcal{B})| = O\left(\sqrt{|\mathcal{A}||\mathcal{B}|q^{3n/2}}\right), \quad a \in \mathbb{F}_q^*, \tag{3.2}$$

which is established in [8] for the character sums

$$S_{\mathbf{f}}(a,\mathcal{A},\mathcal{B}) = \sum_{\mathbf{x}\in\mathcal{A}} \sum_{\mathbf{y}\in\mathcal{B}} \chi(ad_{\mathbf{f}}(\mathbf{x},\mathbf{y})), \quad a \in \mathbb{F}_q, \tag{3.3}$$

where $d_{\mathbf{f}}(\mathbf{x},\mathbf{y})$ is given by (1.5).

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

$$d_{\mathbf{f}}(\mathbf{x},\mathbf{y}) = \lambda, \quad \mathbf{x} \in \mathcal{A},\ \mathbf{y} \in \mathcal{B}. \tag{3.4}$$

As in the proof of Theorem 2.1, using (3.2) instead of (2.4), we deduce

$$\sum_{\lambda\in\mathbb{F}_q} N_{\mathbf{f}}(\lambda)^2 = \frac{1}{q}\sum_{a\in\mathbb{F}_q} |S(a,\mathcal{A},\mathcal{B})|^2 = |\mathcal{A}|^2|\mathcal{B}|^2q^{-1} + O(|\mathcal{A}||\mathcal{B}|q^{3n/2}). \tag{3.5}$$

As before, we also have

$$\sum_{\lambda\in\mathbb{F}_q} N_{\mathbf{f}}(\lambda) = |\mathcal{A}||\mathcal{B}|, \tag{3.6}$$

and by the Cauchy inequality we derive

$$\begin{aligned}(|\mathcal{A}||\mathcal{B}|)^2 = \left(\sum_{\lambda\in\mathbb{F}_q} N(\lambda)\right)^2 &\le \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})\sum_{\lambda\in\mathbb{F}_q} N(\lambda)^2 \\ &< \Gamma(\mathbb{F}_q^n,\mathcal{A},\mathcal{B})\left(|\mathcal{A}|^2|\mathcal{B}|^2q^{-1}+O(|\mathcal{A}||\mathcal{B}|q^{3n/2})\right),\end{aligned} \tag{3.7}$$

which implies the desired result. □

Acknowledgments

The author is very grateful to Alex Iosevich for many useful discussions and encouragement, in particular, for clarifying how the results and methods of [4] can be modified to incorporate the case of distinct sets $\mathcal{A} \neq \mathcal{B}$. During the preparation of this note, the author was supported in part by ARC Grant DP0556431.

References

[1] M. B. Erdogan, *A bilinear Fourier extension theorem and applications to the distance set problem*, International Mathematics Research Notices **2005** (2005), no. 23, 1411–1425.
[2] S. Hofmann and A. Iosevich, *Circular averages and Falconer/Erdös distance conjecture in the plane for random metrics*, Proceedings of the American Mathematical Society **133** (2005), no. 1, 133–143.
[3] A. Iosevich and I. Łaba, *Distance sets of well-distributed planar point sets*, Discrete & Computational Geometry **31** (2004), no. 2, 243–250.
[4] A. Iosevich and M. Rudnev, *Erdös distance problem in vector spaces over finite fields*, to appear in Transactions of the American Mathematical Society.
[5] ———, *Spherical averages, distance sets, and lattice points on convex surfaces*, preprint, 2005.
[6] N. H. Katz and G. Tardos, *A new entropy inequality for the Erdös distance problem*, Towards a Theory of Geometric Graphs, Contemp. Math., vol. 342, American Mathematical Society, Rhode Island, 2004, pp. 119–126.
[7] R. Lidl and H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Cambridge University Press, Cambridge, 1997.
[8] I. E. Shparlinski, *On some generalisations of the Erdös distance problem over finite fields*, Bulletin of the Australian Mathematical Society **73** (2006), no. 2, 285–292.

Igor E. Shparlinski: Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: igor@ics.mq.edu.au