Finite Fields and Their Applications 37 (2016) 179–192

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

Sets with many pairs of orthogonal vectors over finite fields

Omran Ahmadi *, Ali Mohammadian

School of Mathematics, Institute for Research in Fundamental Sciences (IPM), Tehran, Iran

ARTICLE INFO

Article history:
Received 7 July 2014
Received in revised form 15 August 2015
Accepted 25 September 2015
Available online 11 November 2015
Communicated by Olga Polverino

MSC:
05D05
15A63
11T99

Keywords:
Quadratic forms over finite fields
Extremal set theory
Unit distances problem

ABSTRACT

Let n be a positive integer and $\mathcal{B}$ be a non-degenerate symmetric bilinear form over $\mathbb{F}_q^n$, where q is an odd prime power and $\mathbb{F}_q$ is the finite field with q elements. We determine the largest possible size of a subset S of $\mathbb{F}_q^n$ such that $|\{\mathcal{B}(\boldsymbol{x}, \boldsymbol{y}) \mid \boldsymbol{x}, \boldsymbol{y} \in S \text{ and } \boldsymbol{x} \neq \boldsymbol{y}\}| = 1$. We also pose some conjectures concerning nearly orthogonal subsets of $\mathbb{F}_q^n$ where a nearly orthogonal subset T of $\mathbb{F}_q^n$ is a set of vectors in which among any three distinct vectors there are two vectors $\boldsymbol{x}$, $\boldsymbol{y}$ so that $\mathcal{B}(\boldsymbol{x}, \boldsymbol{y}) = 0$.

1. Introduction

Erdős in [6] posed his two famous distinct distances and unit distances problems for the plane and later in [7] he considered the extension of these problems to the d-dimensional Euclidean space. The distinct distances problem asks for $f_d(n)$, the minimum number

* Corresponding author.
E-mail addresses: oahmadid@ipm.ir (O. Ahmadi), ali_m@ipm.ir (A. Mohammadian).

http://dx.doi.org/10.1016/j.ffa.2015.09.009

of distinct distances among n points in the d-dimensional Euclidean space, and the unit distances problem asks for $g_d(n)$, the maximum number of the unit distances that can occur among n points in the d-dimensional Euclidean space. He conjectured that there are two positive constants c_1 and c_2 such that

$$f_2(n) > c_1 \frac{n}{\sqrt{\log n}} \text{ and } f_d(n) > c_2 n^{2/d},$$

for any large enough n and any $d \geqslant 3$. Recently, Katz and Guth in [12] came close to settling this conjecture for the plane by proving

$$f_2(n) > c\frac{n}{\log n},$$

for a positive constant c and any large enough n. Considering $g_d(n)$, the case $d \geqslant 4$ is easier to handle than the cases $d = 2$ and $d = 3$. In some cases it is possible to give exact value of $g_d(n)$. For example, Erdős [7] showed that if $d \geqslant 4$ is even and $n \equiv 0 \pmod{2d}$, then

$$g_d(n) = \frac{n^2(d-2)}{8} + n,$$

for any n large enough dependent on d.

Recently, there has been a growing interest in the q-analogues of the above problems, see [4,13–17] for example. By q-analogue problems we mean that, instead of considering the points in the Euclidean spaces, one can consider points in the n-dimensional vector space over $\mathbb{F}_q$ and ask appropriate and similar questions, where $\mathbb{F}_q$ is the finite field with q elements. For instance, Iosevich and Rudnev in [16] defined the distance between two points $\boldsymbol{x} = (x_1, \ldots, x_n)$ and $\boldsymbol{y} = (y_1, \ldots, y_n)$ in $\mathbb{F}_q^n$ to be $(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2$ and proved that if q is an odd prime power and S is a subset of $\mathbb{F}_q^n$ with $|S| \geqslant cq^{(n+1)/2}$ for a sufficiently large constant c, then the set of distances determined by pairs of distinct points in S contains $\mathbb{F}_q \setminus \{0\}$. Of course, one can change the definition of distance used in [16] using an arbitrary quadratic form over $\mathbb{F}_q^n$ and ask questions analogous to the distinct distances and unit distances problems.

In this article, we are interested in a q-analogue variant of the unit distances problem as follows. Consider $t \in \mathbb{F}_q$ and assume that $\mathcal{B}$ is a non-degenerate symmetric bilinear form over $\mathbb{F}_q^n$. We determine the largest possible cardinality of a subset S of $\mathbb{F}_q^n$ so that $\mathcal{B}(\boldsymbol{x}, \boldsymbol{y}) = t$, for every distinct vectors $\boldsymbol{x}, \boldsymbol{y} \in S$.

There are some results in the literature related to the special case of $t = 0$. Zame in [21] found the largest possible cardinality of a subset $S \subseteq \mathbb{F}_p^n$, for a prime number p, so that the standard coordinate-wise inner product of every two distinct vectors in S is 0. In [20], the general case of non-degenerate symmetric bilinear forms with $t = 0$ has been treated. Unfortunately, main result of [20] contains an error and although it is claimed that upper bounds obtained in [20] are tight, they are actually not. Our Theorem 4 corrects the mistake of [20] by establishing sharp upper bounds.