Canad. Math. Bull. Vol. **55** (2), 2012 pp. 418–423
http://dx.doi.org/10.4153/CMB-2011-160-x

Maximal Sets of Pairwise Orthogonal Vectors in Finite Fields

Le Anh Vinh

Abstract. Given a positive integer n, a finite field $\mathbb{F}_q$ of q elements (q odd), and a non-degenerate symmetric bilinear form B on $\mathbb{F}_q^n$, we determine the largest possible cardinality of pairwise B-orthogonal subsets $\mathcal{E} \subseteq \mathbb{F}_q^n$, that is, for any two vectors $x, y \in \mathcal{E}$, one has $B(x, y) = 0$.

1 Introduction

In this short note, we study the largest possible cardinality of pairwise orthogonal subsets in vector spaces over finite fields. Let n be a positive integer, and let $\mathbb{F}_q$ be the finite field of q elements, where q is an odd prime power. To put the problem in a more general setting, instead of using the usual dot product, we consider each non-degenerate symmetric bilinear form B on $\mathbb{F}_q^n$ (that is, $B(u, v) = B(v, u)$ for all $u, v \in \mathbb{F}_q^n$). Given two n-dimensional vectors $x = (x_1, \dots, x_n)$ and $y = (y_1, \dots, y_n) \in \mathbb{F}_q^n$, if $B(x, y) = 0$, we say that x and y are B-orthogonal, or orthogonal for short when B is clear from the context. Any non-degenerate bilinear form on $\mathbb{F}_q^n$ (q odd) can be given by

$$B(x, y) = \sum_{i=1}^{n} a_i x_i y_i,\ a_i \neq 0, 1 \leq i \leq n, \quad x = (x_1, \dots, x_n), \quad y = (y_1, \dots, y_n) \in \mathbb{F}_q^n. \tag{1.1}$$

Let χ be the quadratic character of $\mathbb{F}_q$. We define $\chi(B) \in \{\pm 1\}$ as

$$\chi(B) = \prod_{i=1}^{n} \chi(a_i).$$

The main result of this short note is the following theorem.

Theorem 1.1 *For any non-degenerate symmetric bilinear form B on $\mathbb{F}_q^n$, we define $I(B, \mathbb{F}_q^n)$ as the largest possible cardinality of pairwise B-orthogonal subsets $\mathcal{E} \subseteq \mathbb{F}_q^n$.*

(i) *If n is odd, then $I(B, \mathbb{F}_q^n) = q^{(n-1)/2} + (n+1)/2$.*
(ii) *If n is even and $\chi(B) = \chi(-1)^{n/2}$, then $I(B, \mathbb{F}_q^n) = q^{n/2} + n/2$.*
(iii) *If n is even and $\chi(B) = -\chi(-1)^{n/2}$, then $I(B, \mathbb{F}_q^n) = q^{n/2-1} + n/2 + 1$.*

Received by the editors March 31, 2009.
Published electronically September 15, 2011.
AMS subject classification: **05B25**.
Keywords: orthogonal sets, zero-distance sets.

Recall that, for a given symmetric bilinear form B, we can define the quadratic form $Q\colon \mathbb{F}_q^n \to \mathbb{F}_q$ by $Q(v) = B(v, v)$; and for any given quadratic form Q, we can pull out a symmetric bilinear form defined by $B(u, v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$. In particular, if $B(\,\cdot\,,\,\cdot\,)$ is given in (1.1), then $Q(x) = \sum_{i=1}^{n} a_i x_i^2$. Similarly, we define $\chi(Q) = \prod_{i=1}^{n} \chi(a_i)$. Iosevich, Shparlinski, and Xiong ([1]) obtained the following results using exponential sum estimates.

Theorem 1.2 ([1, Theorem 1.2]) *For any non-degenerate quadratic form Q on $\mathbb{F}_q^n$, let $I_0(Q, \mathbb{F}_q^n)$ denote the largest possible cardinality of subsets of $\mathcal{E} \subseteq \mathbb{F}_q^n$ with pairwise zero Q-distance; that is, for any two points $x, y \in \mathcal{E}$, one has $Q(x - y) = 0$.*

(i) *If n is odd, then $I_0(Q, \mathbb{F}_q^n) = q^{(n-1)/2}$.*

(ii) *If n is even and $\chi(Q) = \chi(-1)^{n/2}$, then $I_0(Q, \mathbb{F}_q^n) = q^{n/2}$.*

(iii) *If n is even and $\chi(Q) = -\chi(-1)^{n/2}$, then $I_0(Q, \mathbb{F}_q^n) = q^{n/2-1}$.*

We will give another proof of this theorem in this note, which uses only simple linear algebra.

Note that in the Euclidean space $\mathbb{R}^n$, the maximal sets of pairwise orthogonal vectors are simply orthogonal bases of $\mathbb{R}^n$, and the maximal sets of pairwise zero-distance sets are just single-point sets. However, the arithmetic of finite fields allows a richer orthogonal structure. Another example of this phenomenon is the question, which was first studied by Iosevich and Senger [2], of whether a sufficiently large subset of $\mathbb{F}_q^n$ contains a k-tuple of mutually orthogonal vectors. This problem does not have a direct analog in Euclidean or integer geometries because placing the set strictly inside $\{x \in \mathbb{R}^d : x_i > 0\}$ immediately guarantees that no orthogonal vectors are present. On the the other hand, Iosevich and Senger ([2]) showed that if $\mathcal{E} \subset \mathbb{F}_q^n$ of cardinality

$$|\mathcal{E}| \geq Cq^{n\frac{k-1}{k} + \frac{k-1}{2} + \frac{1}{k}}$$

with a sufficiently large constant $C > 0$, then $\mathcal{E}$ contains $(1 + o(1))|\mathcal{E}|^k q^{-\binom{k}{2}}$ k-tuples of k mutually orthogonal vectors in E (see also [6], where the author improved the bound on the cardinality of $\mathcal{E}$ to $|\mathcal{E}| \geq Cq^{\frac{n}{2}+k-1}$ using graph theoretic methods).

2 Maximal Subspaces in Quadratic Hypersurfaces

Since any non-degenerate quadratic form on $\mathbb{F}_q^d$ (q odd) can be diagonalized ([5, Theorem 3.1]), we may assume that Q is given by

$$Q(x) = \sum_{i=1}^{n} a_i x_i^2, : a_i \neq 0, 1 \leq i \leq n,\ x = (x_1, \dots, x_n) \in \mathbb{F}_q^n.$$

We fix a non-square element $\lambda \in \mathbb{F}_q^*$, then it is well known that (see, for example, [1, 4]) any non-degenerate quadratic form Q on $\mathbb{F}_q^n$ can be reduced (by repeated change of variables) to one of the forms $Q_{n,\varepsilon}$, $\varepsilon \in \{1, \lambda\}$, depending on the value of $\chi(Q)$, where for $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$, if $n = 2m$ is even, then

$$Q_{n,\varepsilon}(x) = x_1^2 - x_2^2 + x_3^2 - x_4^2 + \cdots + x_{2m-1}^2 - \varepsilon x_{2m}^2, \tag{2.1}$$

https://doi.org/10.4153/CMB-2011-160-x Published online by Cambridge University Press

and if $n = 2m + 1$ is odd, then

$$Q_{n,\varepsilon}(x) = x_1^2 - x_2^2 + \cdots + x_{2m-1}^2 - x_{2m}^2 + \varepsilon x_{2m+1}^2.$$

For any non-degenerate quadratic form Q on $\mathbb{F}_q^n$, let S_Q denote the quadratic hypersurface associated with Q on $\mathbb{F}_q^d$, that is

$$S_Q = \{x \in \mathbb{F}_q^d : Q(x) = 0\}.$$

The following lemma tells us about the maximal dimension of linear subspaces in S_Q.

Lemma 2.1 *Let W be a linear subspace of maximal dimension in S_Q.*

(i) *If n is odd, then* $\dim(W) = (n-1)/2$.
(ii) *If n is even and $\chi(Q) = \chi(-1)^{n/2}$, then* $\dim(W) = n/2$.
(iii) *If n is even and $\chi(Q) = -\chi(-1)^{n/2}$, then* $\dim(W) = n/2 - 1$.

Proof Let $(\mathbb{F}_q^n)^*$ be the dual space of $\mathbb{F}_q^n$, that is, the space of all linear functionals on $\mathbb{F}_q^n$. Recall that a symmetric bilinear form B is associated with the corresponding linear map $\widetilde{Q}\colon \mathbb{F}_q^n \to (\mathbb{F}_q^n)^*$ given by sending v to the linear form $B(v, \cdot)$, where

$$B(u,v) = \tfrac{1}{2}\big(Q(u+v) - Q(u) - Q(v)\big). \tag{2.2}$$

Let W be a linear subspace in S_Q, then $Q|_W = 0$, or equivalently $\widetilde{Q}(W) \subset \operatorname{Ann}(W)$. Since Q is non-degenerate, $\widetilde{Q}$ is an isomorphism. So we have

$$\dim(W) \leq \dim(\operatorname{Ann}(W)) = \dim(\mathbb{F}_q^n) - \dim(W),$$

which implies that

$$\dim(W) \leq n/2. \tag{2.3}$$

For $1 \leq i \leq n$, denote by e_i the vector in $\mathbb{F}_q^n$ with 1 in the i-th entry and 0 everywhere else. Suppose that $n = 2m+1$. Let $W = \operatorname{span}\{e_1 + e_2, \ldots, e_{2m-1} + e_{2m}\}$, then $\dim(W) = (n-1)/2$ and $W \subset S_Q$. This proves the first claim of the lemma.

Suppose that $n = 2m$ and $\chi(Q) = \chi(-1)^{n/2}$. By the classification of non-degenerate quadratic forms on $\mathbb{F}_q^n$, we assume that $Q = Q_{n,1}$ (given in (2.1)). Let $W = \operatorname{span}\{e_1 + e_2, \ldots, e_{2m-1} + e_{2m}\}$, then $\dim(W) = n/2$ and $W \subset S_Q$. This proves the second claim of the lemma.

Next, we suppose that $n = 2m$ and $\chi(Q) = -\chi(-1)^{n/2}$. Let $O(\mathbb{F}_q^n, Q)$ be the group of all linear transformations on $\mathbb{F}_q^n$ that fix Q (which is called the orthogonal group associated with the quadratic form Q). We will need the following lemma.

Lemma 2.2 *Let W and V be any two linear subspaces of dimension k on $\mathbb{F}_q^n$, and let $\{w_1, \ldots, w_k\}$ and $\{v_1, \ldots, v_k\}$ be orthogonal bases of W and V, respectively. Suppose that $\|w_i\| = \|v_i\|$, $1 \leq i \leq k$, then there exists an orthogonal transformation $O \in O(\mathbb{F}_q^n, Q)$ such that $O(W) = V$.*

https://doi.org/10.4153/CMB-2011-160-x Published online by Cambridge University Press

Proof Let $\{w_1, \dots, w_k\}$ and $\{v_1, \dots, v_k\}$ be basis of W and V, respectively. It suffices to show that there exists an orthogonal transformation $O \in O(\mathbb{F}_q^n, Q)$ such that $O(w_i) = v_i$, $i = 1, \dots, k$. The proof of this claim proceeds by induction. The base case $k = 1$ follows immediately from the fact that the orthogonal group with respect to Q acts transitively on S_Q. Suppose that the claim holds for $k-1$; we show that it also holds for k. Since $\|w_1\| = \|v_1\|$, there exists an orthogonal transformation Q_1 that maps w_1 to v_1. Let $w_2', \dots, w_k'$ be images of $w_2, \dots, w_k$ under this map. Set $W' = \operatorname{span}\{w_2', \dots, w_k'\}$ and $V' = \operatorname{span}\{v_2, \dots, v_k\}$, then W' and V' are two linear subspaces of dimension $k-1$ on $v_1^{\perp} \cong \mathbb{F}_q^{n-1}$. Note that $\|w_i'\| = \|v_i\|$ for $2 \le i \le k$. Hence, it follows from the induction hypothesis that there exists an affine, orthogonal transformation O' on $v_1^{\perp} \cong \mathbb{F}_q^{n-1}$ such that $O'(W') = V'$. Let $O = O' \circ Q'$. This concludes the proof of the induction step and the proof of Lemma 2.2. ∎

Continuing the proof of Lemma 2.1, let $W = \operatorname{span}\{e_1 + e_2, \dots, e_{2n-3} + e_{2n-2}\}$, then $\dim(W) = n/2 - 1$ and $W \subset S_Q$. Suppose that S_Q contains a linear subspace of dimension $n/2$. It follows from Lemma 2.2 that there exists an $n/2$-dimensional linear subspace W of S_Q such that $W' \subseteq W$. Choose any $v = (v_1, \dots, v_n) \in W$ such that $v \in (W')^{\perp}$. Since $v \in (e_{2i-1} + e_{2i})^{\perp}$ $(1 \le i \le n/2 - 1)$, we have $v_{2i-1} = -v_{2i}$ for $i = 1, \dots, n/2 - 1$. Note that $v \in S_Q$, so $v_{2n-1}^2 - \lambda v_{2n}^2 = 0$. It follows that $v_{2n-1} = v_{2n} = 0$ or $v \in W'$, which is a contradiction. The third claim of Lemma 2.1 follows. ∎

3 Maximal Pairwise Orthogonal Sets

We are now ready to give a proof of Theorem 1.1. Let W_0 be the maximal linear subspace of S_Q given in the proof of Lemma 2.1. Let W_1 be an orthogonal basis of $W_0^{\perp}$. It is clear that $\mathcal{E} = W_0 \cup W_1$ is a pairwise orthogonal set. This completes the proof of the lower bounds.

Next, we prove the upper bounds. Let $\mathcal{E}$ be a pairwise orthogonal set of maximal cardinality. Set $\mathcal{E}_0 = \mathcal{E} \cap S_Q$ and $\mathcal{E}_1 = \mathcal{E} \setminus \mathcal{E}_0$. Note that if $x \in \mathcal{E}_0$, then $B(x, x) = 0$. Hence, for any $x, y \in \mathcal{E}_0, z \in \mathcal{E}$, and $\lambda_1, \lambda_2 \in \mathbb{F}_q$, one has

$$B(\lambda_1 x + \lambda_2 y, z) = \lambda_1 B(x, z) + \lambda_2 B(y, z) = 0.$$

By the maximality of $\mathcal{E}$, we have $\lambda_1 x + \lambda_2 y \in \mathcal{E}_0$. This implies that $\mathcal{E}_0$ is a linear subspace of S_Q. Suppose that $x_0 = \sum \alpha_i x_i$ for some $x_0, x_1, \dots, x_k \in \mathcal{E}_1, \alpha_1, \dots, \alpha_k \in \mathbb{F}_q$. Then

$$B(x_0, x_0) = \sum_{i=1}^{k} \alpha_i B(x_i, x_0) = 0,$$

which is a contradiction. Hence, $\mathcal{E}_1$ is a linearly independent set. It follows that

$$|\mathcal{E}| = |\mathcal{E}_0| + |\mathcal{E}_1| \le |\mathcal{E}_0| + (n - \dim(\mathcal{E}_0)). \tag{3.1}$$

The upper bounds follow immediately from (3.1) and Lemma 2.1. This completes the proof of Theorem 1.1. ∎

4 Maximal Pairwise Zero-Distance Sets

We recall the following lemma, which is due to Iosevich, Shparlinski, and Xiong [1]. Since the proof of this lemma is short and easy, we will reproduce it here for the sake of completeness.

Lemma 4.1 *If $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a maximal subset with pairwise zero Q-distance and $0 \in \mathcal{E}$, then $\mathcal{E}$ is a linear subspace of S_Q.*

Proof Suppose that $\mathcal{E} \subseteq \mathbb{F}_q^n$ is a maximal subset with pairwise zero Q-distance and $0 \in \mathcal{E}$. For any $x \in \mathcal{E}$, one has $Q(x) = Q(x-0) = 0$. Hence, $\mathcal{E} \subset S_Q$. For any $x, y \in \mathcal{E}$, one has

$$B(x,y) = \tfrac{1}{2}\big(Q(x-y) - Q(x) - Q(y)\big) = 0.$$

Therefore, for any $x, y, z \in \mathcal{E}$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q$,

$$\begin{aligned} &Q(\lambda_1 x + \lambda_2 y - z) \\ &\quad = \lambda_1^2 Q(x) + \lambda_2^2 Q(y) + Q(z) + 2\lambda_1\lambda_2 B(x,y) - 2\lambda_1 B(x,z) - 2\lambda_2 B(y,z) \\ &\quad = 0. \end{aligned}$$

By the maximality of $\mathcal{E}$, we have $\lambda_1 x + \lambda_2 y \in \mathcal{E}$. This implies that $\mathcal{E}$ is a linear subspace of S_Q and concludes the proof of the lemma. ∎

Theorem 1.2 now follows immediately from Lemmas 2.1 and 4.1.

5 Remarks

Note that the upper bound (2.3) in the proof of Lemma 2.1 can also be obtained by a simple character sum estimate. We will need the following estimate of a character sum with bilinear forms over finite fields.

Lemma 5.1 *Let $B(\cdot,\cdot)$ be a non-degenerate bilinear form in the n-dimensional vector space $\mathbb{F}_q^n$, and ψ be a non-trivial additive character on $\mathbb{F}_q$. For any two sets $\mathcal{E}, \mathcal{F} \subset \mathbb{F}_q^n$ with $|\mathcal{E}| = E$, $|\mathcal{F}| = F$, we have*

$$\Big|\sum_{u\in\mathcal{E}, v\in\mathcal{F}} \psi\big(B(u,v)\big)\Big| \leqslant \sqrt{q^n|\mathcal{E}||\mathcal{F}|}.$$

Proof Viewing $\sum_{u\in\mathcal{E},v\in\mathcal{F}} \psi(B(u,v))$ as a sum in v, applying the Cauchy-Schwarz inequality, and dominating the sum over $v \in \mathcal{F}$ by the sum over $v \in \mathbb{F}_q^n$, we see that

$$\begin{aligned} \Big|\sum_{u\in\mathcal{E}, v\in\mathcal{F}} \psi\big(B(u,v)\big)\Big|^2 &\leqslant |\mathcal{F}| \sum_{v\in\mathbb{F}_q^n} \sum_{u,u'\in\mathcal{E}} \psi\big(B(u-u',v)\big) \\ &\leqslant |\mathcal{F}| \sum_{u,u'\in\mathcal{E}} \sum_{v\in\mathbb{F}_q^n} \psi(B(u-u',v)) \\ &\leqslant q^n|\mathcal{E}||\mathcal{F}|, \end{aligned}$$

since the inner sum over v vanishes unless $u = u'$. ∎

https://doi.org/10.4153/CMB-2011-160-x Published online by Cambridge University Press

Suppose that W is a linear subspace in S_Q. It follows from (2.2) that $B(u,v) = 0$ for any $u, v \in W$. Hence,

$$|W|^2 = \Big| \sum_{u,v \in W} \psi\big(B(u,v)\big) \Big| \leqslant q^{n/2}|W|,$$

or equivalently, $\dim(W) \leq n/2$.

References

[1] A. Iosevich, I. Shparlinski, and M. Xiong, *Sets with integral distances in finite fields.* Trans. Amer. Math. Soc. **362**(2010), no. 4, 2189–2204. http://dx.doi.org/10.1090/S0002-9947-09-05004-1

[2] A. Iosevich and S. Senger, *Orthogonal systems in vector spaces over finite fields.* Electron. J. Combin. **15**(2008), no. 1, Research Paper 151.

[3] S. Kurz, *Integral point sets over finite fields.* Australas. J. Combin. **43**(2009), 3–29.

[4] W. M. Kwok, *Character tables of association schemes of affine type.* European J. Combin. **13**(1992), no. 3, 167–185. http://dx.doi.org/10.1016/0195-6698(92)90022-R

[5] S. Lang, *Algebra.* Revised third ed., Graduate Texts in Mathematics, 211, Springer-Verlag, New York, 2002.

[6] L. A. Vinh, *On the number of orthogonal systems in vector spaces over finite fields.* Electron. J. Combin. **15**(2008), no. 1, Note 32.

Mathematics Department, Harvard University, Cambridge, MA, 02138, USA
e-mail: vinh@math.harvard.edu

https://doi.org/10.4153/CMB-2011-160-x Published online by Cambridge University Press