Symmetric bilinear forms over finite fields of even characteristic

Kai-Uwe Schmidt

12 November 2008 (revised 15 May 2010)

Abstract

Let S_m be the set of symmetric bilinear forms on an m-dimensional vector space over $\mathrm{GF}(q)$, where q is a power of two. A subset Y of S_m is called an (m,d)-set if the difference of every two distinct elements in Y has rank at least d. Such objects are closely related to certain families of codes over Galois rings of characteristic four. An upper bound on the size of (m,d)-sets is derived, and in certain cases, the rank distance distribution of an (m,d)-set is explicitly given. Constructions of (m,d)-sets are provided for all possible values of m and d.

1 Introduction

Consider the set S_m of symmetric bilinear forms on an m-dimensional vector space over $K = \mathrm{GF}(q)$, where q is a power of two. We study subsets Y of S_m having the property that for all distinct $B, C \in Y$ we have $\mathrm{rank}(B - C) \geq d$ for fixed integer d. Such subsets will be called (m,d)-*sets*. In particular, for given m and d, we are interested in (m,d)-sets containing as many elements as possible.

Two similar problems have been studied in the 1970s. Delsarte [Del78] considered sets of unrestricted bilinear forms, and Delsarte and Goethals [DG75] studied sets of alternating bilinear forms (both studies apply in fact to fields of arbitrary characteristic). These references make heavy use of the fact that the sets of unrestricted and alternating bilinear forms give rise to distance-regular graphs (with the distance defined by the rank), and therefore, the powerful theory of association schemes can be applied. In contrast, the graph naturally associated with symmetric bilinear forms is not distance regular (see [BCN89, Sec. 9.5.D], for example).

Let A_m denote the set of alternating bilinear forms on an m-dimensional vector space over K. Our main tools, introduced in Section 2, are two mappings ϕ and ψ from S_m to A_{m+1} and A_m, respectively. The crucial property of these mappings is that they act, in some sense, rank preserving. Given an (m,d)-set Y, we then study the images $\phi(Y)$ and $\psi(Y)$, which allows us to apply the theory of association schemes again. This approach is used in Section 3 to derive a bound on the size of (m,d)-sets, which turns out to be tight for odd d and for $d = m$. Moreover, if Y is a subgroup of S_m and $\phi(Y)$ is a t-design (according to Delsarte [Del73]) for some $t \geq (m-d)/2$, then the rank distribution of Y is explicitly given. In Section 4 we provide constructions of (m,d)-sets

Kai-Uwe Schmidt is with Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby BC V5A 1S6, Canada. He is supported by Deutsche Forschungsgemeinschaft (German Research Foundation) under Research Fellowship SCHM 2609/1-1. Email: kuschmidt@sfu.ca.

being subgroups of S_m. When d is odd and when $d = m$, these constructions yield optimal sets in the sense that their size is as large as it can be. Except when m is odd and d is even, the rank distance distributions of our constructed sets can be obtained from the results of Section 3.

The theories developed by Delsarte [Del78] and Delsarte and Goethals [DG75] have found applications in classical coding theory. In particular, since each K-valued alternating bilinear form is associated with a K-valued quadratic form, [DG75] gives rise to several interesting subcodes of the second-order Reed–Muller code, including the Kerdock code and the chain of Delsarte–Goethals codes (see [MS77, Ch. 15], for example). The present study was motivated by the fact that every K-valued symmetric bilinear form is associated with an R-valued quadratic form, where R is the Galois ring of size q^2 and characteristic 4 (see [Bro72], [Woo93] for $R = \mathbb{Z}_4$ and [LDR07] for the general case). R-valued quadratic forms, derived from (m, m)-sets, have been used to construct Kerdock codes over R, which can be mapped back to K by a distance-preserving map (see [CCKS97] for $R = \mathbb{Z}_4$ and [GMR07] for the general case). Further connections of (m, d)-sets to codes over $\mathbb{Z}_4$ and to $\mathbb{Z}_4$-valued sequence sets with mutually low correlation are reported in [Sch09].

2 Bilinear Forms

2.1 Sets of Bilinear Forms

Let $K = \mathrm{GF}(q)$ be the finite field of q elements, where q is a power of 2. Let V and W be vector spaces over K with $\dim_K(V) = m$ and $\dim_K(W) = k$. Without loss of generality, we shall assume that $m \le k$. A *bilinear form* is a mapping $B : V \times W \to K$ satisfying

$$B\left(\sum_i a_i x_i, \sum_j b_j y_j\right) = \sum_i \sum_j a_i b_j B(x_i, y_j) \quad \text{for all } a_i, b_j \in K,\ x_i \in V,\ y_j \in W.$$

If V' and W' are subspaces of V and W, respectively, then $B|_{V' \times W'}$ denotes the bilinear form that is induced on $V' \times W'$ by B.

Let $\{\xi_1, \xi_2, \ldots, \xi_m\}$ and $\{\zeta_1, \zeta_2, \ldots, \zeta_k\}$ be bases for V and W over K, respectively. Then, relative to these bases, the bilinear form B is uniquely determined by the matrix of size $m \times k$

$$B = (b_{ij})_{1 \le i \le m,\, 1 \le j \le k}, \quad \text{where} \quad b_{ij} = B(\xi_i, \zeta_j). \tag{1}$$

The *left radical* $\mathrm{rad}(B)$ of the bilinear form B is defined as the set of all $x \in V$ such that $B(x, y) = 0$ for all $y \in W$. The *rank* of B is defined to be

$$\mathrm{rank}(B) := \dim_K(V) - \dim_K(\mathrm{rad}(B)).$$

Note that the rank of B is precisely the rank of its associated matrix (1).

A *symmetric* bilinear form on V is a bilinear form $B : V \times V \to K$ that satisfies symmetry:

$$B(x, y) = B(y, x) \quad \text{for all } x, y \in V.$$

Letting $\xi_i = \zeta_i$ for $i = 1, 2, \ldots, m$, we conclude from (1) that a matrix associated with a symmetric bilinear form is symmetric. Hence, after fixing a basis for V over K, there is a one-to-one correspondence between symmetric bilinear forms on V and $m \times m$ symmetric matrices over K. The

set of symmetric bilinear forms on V will be denoted by S_m. For later reference, we note that $|S_m| = q^{m(m+1)/2}$.

An *alternating* bilinear form on V is a bilinear form $B : V \times V \to K$ that satisfies

$$B(x, x) = 0 \quad \text{for each } x \in V.$$

It is known that the rank of an alternating bilinear form is always even (see [DG75, Lem. 10], for example). Observe that $B(x, x) = 0$ for each $x \in V$ forces $B(x, y) + B(y, x) = 0$. Thus, since the characteristic of K is even, every such alternating bilinear form is also symmetric. Letting $\xi_i = \zeta_i$ for $i = 1, 2, \ldots, m$ in (1), the corresponding matrix of an alternating bilinear form on V is an $m \times m$ alternating matrix over K (that is, a symmetric matrix over K with zero main diagonal). We shall denote the set of alternating bilinear forms on V by A_m. Note that $|A_m| = q^{m(m-1)/2}$.

We are interested in subsets $Y \subseteq S_m$ having the property

$$\operatorname{rank}(B - C) \geq d \quad \text{for all distinct } B, C \in Y$$

and for fixed integer d. We call such a subset an (m, d)-*set*. If, in addition, every $B \in Y$ is alternating, the set Y is called an *alternating* (m, d)-*set*. We say that Y is *additive* if Y is a subgroup of S_m.

The *distance distribution* of Y is the $(m + 1)$-tuple $(b_0, b_1, \ldots, b_m)$, where

$$b_i = \frac{1}{|Y|} \big| \{(B, C) \in Y \times Y : \operatorname{rank}(B - C) = i\} \big|.$$

Clearly, for every (m, d)-set Y, we have

$$b_i = 0 \quad \text{for each } i = 1, 2, \ldots, d - 1.$$

The *rank distribution* of Y is the $(m+1)$-tuple $(a_0, a_1, \ldots, a_m)$, where a_i is the number of elements in Y of rank i. The subset Y is called *distance invariant* if $a_i = b_i$ for each $i = 0, 1, \ldots, m$. In particular, every additive set is distance invariant.

2.2 The Association Scheme of Alternating Bilinear Forms

In what follows, we recall some facts about the association scheme of alternating bilinear forms that are relevant for this paper. More background of association schemes in general can be found, for example, in [BI84], [Del73], [DL98]. For details of the association scheme of alternating bilinear forms we refer to [DG75].

Throughout this section let $n := \lfloor \frac{m}{2} \rfloor$. We define the following relations

$$R_i = \{(B, C) \in A_m \times A_m : \operatorname{rank}(B - C) = 2i\} \quad \text{for } i = 0, 1, \ldots, n,$$

and write $R = (R_0, R_1, \ldots, R_n)$. Then (A_m, R) is the *association scheme of alternating bilinear forms*. This is a self-dual metric association scheme with n classes. Let $((D_i)_{u,v})_{u,v \in A_m}$ be the incidence matrix of R_i, that is,

$$(D_i)_{u,v} = \begin{cases} 1 & \text{if } (u, v) \in R_i \\ 0 & \text{otherwise.} \end{cases}$$

Then $\{D_0, D_1, \ldots, D_n\}$ is a basis for a real vector space of symmetric matrices, called the *Bose–Mesner algebra* of (A_m, R). It is a consequence of a general property of association schemes that, for this vector space, there exists another uniquely defined basis $\{J_0, J_1, \ldots, J_n\}$, consisting of minimal idempotent matrices given by

$$J_k = \frac{1}{|A_m|} \sum_{i=0}^{n} q_k(i) D_i. \tag{2}$$

The numbers $q_k(i)$ $(i, k = 0, 1, \ldots, n)$ are the Q (and P)-eigenvalues of the scheme (A_m, R). These numbers were determined in [DG75] and are best expressed in terms of Gaussian binomial coefficients. Once and for all we define $p := q^2$ and, for real x and nonnegative integer k, denote by $\begin{bmatrix} x \\ k \end{bmatrix}$ the *p-binomial coefficient*, which is given by $\begin{bmatrix} x \\ k \end{bmatrix} = \prod_{i=1}^{k} (p^{x-i+1} - 1)/(p^i - 1)$. Elementary properties of p-binomial coefficients can be found, for example, in [And76] and [DG75]. From [DG75, Eq. (15)] we have

$$q_k(i) = \sum_{j=0}^{k} (-1)^{k-j} p^{\binom{k-j}{2}} \begin{bmatrix} n-j \\ n-k \end{bmatrix} \begin{bmatrix} n-i \\ j \end{bmatrix} Q^j \quad \text{for } i, k = 0, 1, \ldots, n,$$

where $Q := q^{m(m-1)/2n}$. Equivalently, the numbers $q_k(i)$ can be defined via the $n+1$ equations

$$\sum_{k=0}^{j} \begin{bmatrix} n-k \\ n-j \end{bmatrix} q_k(i) = \begin{bmatrix} n-i \\ j \end{bmatrix} Q^j \quad \text{for } j = 0, 1, \ldots, n \tag{3}$$

(see [DG75, Eq. (29)]).

Now let Y be a subset of A_m, and let $(a_0, a_1, \ldots, a_m)$ and $(b_0, b_1, \ldots, b_m)$ be the rank and distance distribution of Y, respectively. Note that $a_i = b_i = 0$ if i is odd. The *dual rank distribution* of Y is defined to be the $(n+1)$-tuple $(a'_0, a'_1, \ldots, a'_n)$, where

$$a'_k = \sum_{i=0}^{n} q_k(i) a_{2i}. \tag{4}$$

Similarly, the *dual distance distribution* of Y is the $(n+1)$-tuple $(b'_0, b'_1, \ldots, b'_n)$, where

$$b'_k = \sum_{i=0}^{n} q_k(i) b_{2i}. \tag{5}$$

Note that we have

$$a'_0 = b'_0 = |Y|. \tag{6}$$

We shall need the following lemma relating the dual rank and dual distance distributions.

Lemma 1. *Let Y be a subset of A_m, and suppose that Y contains the zero form. Let $(a'_0, a'_1, \ldots, a'_n)$ and $(b'_0, b'_1, \ldots, b'_n)$ be the dual rank and dual distance distribution of Y, respectively. Then*

$$b'_k = 0 \Longrightarrow a'_k = 0 \quad \textit{for each } k = 0, 1, \ldots, n.$$

Proof. Let $\chi = (\chi_u)_{u \in A_m}$ be the incidence vector of Y, that is,

$$\chi_u = \begin{cases} 1 & \text{if } u \in Y \\ 0 & \text{otherwise.} \end{cases}$$

By convention, we order the elements in A_m such that the ordering starts with the zero form. Hence, by assumption, the first element in χ is always equal to one. If $(b_0, b_1, \ldots, b_m)$ is the distance distribution of Y, we have by definition

$$b_{2i} = \frac{1}{|Y|}\chi D_i \chi^T,$$

and by (5) and (2),

$$\begin{aligned} b'_k &= \frac{1}{|Y|}\sum_{i=0}^{n} q_k(i)(\chi D_i \chi^T) \\ &= \frac{1}{|Y|}\chi\left(\sum_{i=0}^{n} q_k(i) D_i\right)\chi^T \\ &= \frac{|A_m|}{|Y|}\chi J_k \chi^T. \end{aligned}$$

Hence, $b'_k = 0$ is equivalent to $\chi J_k \chi^T = 0$.

Now let $(a_0, a_1, \ldots, a_m)$ be the rank distribution of Y, and let d_i be the first row of D_i. Then $a_i = d_i \chi^T$, and similarly as above, $a'_k = |A_m| \cdot j_k \chi^T$, where j_k is the first row of J_k. Since J_k is idempotent, it has eigenvalues 0 or 1, and therefore, J_k is positive semi-definite. This last fact can be used to show that $\chi J_k \chi^T = 0$ is equivalent to $J_k \chi^T = 0$. In particular, the latter implies $j_k \chi^T = 0$ and $a'_k = 0$. □

Delsarte [Del73] defined the notion of a t-design in a general metric association scheme. We quote this definition for the association scheme of alternating bilinear forms.

Definition 2. Let Y be a subset of A_m, and let $(b'_0, b'_1, \ldots, b'_n)$ be its dual distance distribution. Then Y is called a *t-design* if

$$b'_k = 0 \quad \text{for each } k = 1, 2, \ldots, t.$$

A combinatorial interpretation of t-designs in A_m was obtained by Munemasa [Mun86] (see also Stanton [Sta86]).

Theorem 3 (Munemasa [Mun86, Thm. 1])**.** *Let the elements in A_m be defined on the m-dimensional vector space V, and let t be an integer satisfying $0 \le t \le \frac{m-1}{2}$. Then a subset Y of A_m is a t-design if and only if for every $(2t+1)$-dimensional subspace U of V the multiset*

$$\{B|_{U\times U} : B \in Y\}$$

contains each alternating bilinear form on U equally often.

2.3 From Symmetric to Alternating Bilinear Forms

In what follows, we study two mappings from S_m to A_m and A_{m+1}, which will be of crucial importance in our analysis of (m, d)-sets. Let V be an m-dimensional vector space over K. Given a

symmetric bilinear form $B : V \times V \to K$, we associate the following two alternating bilinear forms with B. We define $\psi(B) : V \times V \to K$ by

$$\psi(B)(x, y) := B(x, y) + \sqrt{B(x, x)B(y, y)},$$

and $\phi(B) : (V \times K) \times (V \times K) \to K$ by

$$\phi(B)((x, \alpha), (y, \beta)) := \psi(B)(x, y) + \beta\sqrt{B(x, x)} + \alpha\sqrt{B(y, y)}. \tag{7}$$

Notice that, since the characteristic of K is even, the square root always exists in K.

Once we fix a basis for V over K, ψ and ϕ induce mappings acting on the set of $m \times m$ symmetric matrices over K, which we shall also denote by ψ and ϕ, respectively. Given an $m \times m$ symmetric matrix B over K, it will be useful to have an expression for $\psi(B)$ and $\phi(B)$. To this end, we define $d(B)$ to be a row vector that contains, in the natural order, the square roots of the elements in the main diagonal of B. Then, for a suitably chosen basis for V over K, the $m \times m$ matrix $\psi(B)$ is given by

$$\psi(B) = B + d(B)^T d(B),$$

and the $(m + 1) \times (m + 1)$ matrix $\phi(B)$ is given by

$$\phi(B) = \begin{pmatrix} \psi(B) & d(B)^T \\ d(B) & 0 \end{pmatrix}.$$

In this matrix notation, the mapping ϕ has been previously used in [CCKS97] and [GMR07] as a transition from the set of $m \times m$ symmetric matrices over K to the set of $(m + 1) \times (m + 1)$ alternating matrices over K. Notice that ϕ acts as a bijection from S_m to A_{m+1}.

Next we state some "rank-preserving" properties of ψ and ϕ.

Lemma 4. *For every $B \in S_m$ we have*

$$\operatorname{rank}(\psi(B)) = 2\left\lfloor \frac{\operatorname{rank}(B)}{2} \right\rfloor$$
$$\operatorname{rank}(\phi(B)) = 2\left\lfloor \frac{\operatorname{rank}(B) + 1}{2} \right\rfloor.$$

Proof. It is sufficient to prove the statements in the lemma for B being an $m \times m$ symmetric matrix over K. Let $x \in K^m$ be a row vector. We can write

$$(xd(B)^T)^2 = xBx^T,$$

and therefore have

$$xB = 0 \Longrightarrow xd(B)^T = 0. \tag{8}$$

Hence, if $xB = 0$, then $x\psi(B) = 0$, which implies that the rank of $\psi(B)$ is at most the rank of B. But the ranks of B and $\psi(B)$ can differ by at most one, so that

$$\operatorname{rank}(B) - 1 \leq \operatorname{rank}(\psi(B)) \leq \operatorname{rank}(B).$$

Since $\psi(B)$ has even rank, we have proved the claim for ψ.

Now observe that

$$\begin{pmatrix} x & 0 \end{pmatrix} \phi(B) = \begin{pmatrix} xB + xd(B)^T d(B) & xd(B)^T \end{pmatrix}.$$

From (8) we find that $xB = 0$ forces $(x \;\; 0)\phi(B) = 0$, which implies that the rank of $\phi(B)$ is at most $\mathrm{rank}(B) + 1$. On the other hand, if $xB \neq 0$, then $(x \;\; 0)\phi(B) \neq 0$, so that the rank of $\phi(B)$ is at least the rank of B. In summary,

$$\mathrm{rank}(B) \leq \mathrm{rank}(\phi(B)) \leq \mathrm{rank}(B) + 1,$$

and the claim for ϕ follows since $\phi(B)$ has even rank. □

Lemma 5. *For all $B, C \in S_m$ we have*

$$\mathrm{rank}(\phi(B + C)) = \mathrm{rank}(\phi(B) + \phi(C)).$$

Proof. It is sufficient to prove the assertion in the lemma for B and C being $m \times m$ symmetric matrices over K. Abbreviating $b := d(B)$ and $c := d(C)$, we then have

$$\phi(B + C) = \begin{pmatrix} B + C + (b + c)^T (b + c) & b^T + c^T \\ b + c & 0 \end{pmatrix}$$

and

$$\phi(B) + \phi(C) = \begin{pmatrix} B + C + b^T b + c^T c & b^T + c^T \\ b + c & 0 \end{pmatrix}.$$

Define the matrix

$$R := \begin{pmatrix} I & b^T \\ 0 \cdots 0 & 1 \end{pmatrix},$$

where I is the identity matrix of the same size as B and C. Then it is easy to verify that

$$\phi(B) + \phi(C) = R\phi(B + C)R^T.$$

The lemma follows since R is nonsingular. □

By combining Lemmas 4 and 5 we conclude, for all $B, C \in S_m$,

$$\frac{\mathrm{rank}(\phi(B) + \phi(C))}{2} = \left\lfloor \frac{\mathrm{rank}(B + C) + 1}{2} \right\rfloor. \tag{9}$$

This shows that ϕ has a "distance-preserving" property. We refer to Section 5 for consequences of this fact, which are of independent interest.

For the remainder of this paper we define three mappings acting on an (m, d)-set Y:

$$\begin{aligned} \phi(Y) &:= \{\phi(B) : B \in Y\}, \\ \psi(Y) &:= \{\psi(B) : B \in Y\}, \\ \theta(Y) &:= \{B : B \in Y \wedge B \text{ is alternating}\}. \end{aligned}$$

Since every element in $\theta(Y)$ has even rank, $\theta(Y)$ is an alternating $(m, 2\lfloor \frac{d+1}{2} \rfloor)$-set. By (9), $\phi(Y)$ is an alternating $(m + 1, 2\lfloor \frac{d+1}{2} \rfloor)$-set.

3 Properties of (m, d)-Sets

3.1 An Upper Bound on the Size of (m, d)-Sets

Delsarte and Goethals proved a bound on the size of alternating $(m, 2e)$-sets [DG75, Thm. 4 (i)]. Moreover, if the bound is attained, then the set is automatically an $(\lfloor \frac{m}{2} \rfloor - e + 1)$-design [DG75, Eq. (33)]. We shall summarise these results in the following theorem.

Theorem 6 (Delsarte and Goethals [DG75])**.** *Write $n := \lfloor \frac{m}{2} \rfloor$ and $Q := q^{m(m-1)/2n}$. Then every alternating $(m, 2e)$-set Y satisfies*

$$|Y| \leq Q^{n-e+1}.$$

Moreover, in case of equality, Y is an $(n - e + 1)$-design.

Let Y be an (m, d)-set. Since $\phi(Y)$ is an alternating $(m + 1, 2\lfloor \frac{d+1}{2} \rfloor)$-set by (9), Theorem 6 implies the following.

Corollary 7. *Define $n := \lfloor \frac{m+1}{2} \rfloor$ and $Q := q^{m(m+1)/2n}$. Then every (m, d)-set Y satisfies*

$$|Y| \leq Q^{n-\lfloor \frac{d-1}{2} \rfloor}.$$

Remark 8. (1) The constructions in Section 4 show that the bound on the size of (m, d)-sets is tight for odd d. (2) When d is even, the bound in Corollary 7 cannot be tight, as seen by inspecting Theorem 10 below. Indeed, if $d = m$ and m is even, an improvement of the bound can be obtained as follows. Identify an (m, m)-set Y with a set of $m \times m$ symmetric matrices over K. Then all the matrices in the set must have distinct first rows. Therefore, every (m, m)-set Y satisfies $|Y| \leq q^m$ for either m, which is attained by the constructions given in Section 4. This bound should be compared with the bound $|Y| \leq Q$, given in Corollary 7.

3.2 Rank and Distance Distribution

In this section we compute, under certain conditions, the rank distribution of additive (m, d)-sets and their alternating subsets. We proceed in two steps. In a first step, we prove in Theorem 9 below a result on the rank and distance distribution of subsets of A_m, which generalises a result by Delsarte and Goethals [DG75, Thm. 4 (ii)]. From Theorem 9 we can obtain the distance distribution of the alternating subset $\theta(Y)$ of an (m, d)-set Y provided that $d \geq m - 2t$ and $\theta(Y)$ is a t-design. In a second step, we compute in Theorem 10 below the rank distribution of an additive (m, d)-set Y provided that $d \geq m - 2t$ and $\phi(Y)$ is a t-design. This is accomplished by using Theorem 9 to get the rank distributions of the images $\phi(Y)$ and $\psi(Y)$, which after combination with Lemma 4 give the rank distribution of Y.

Theorem 9. *Let $m > 1$ be an integer, and write $n := \lfloor \frac{m}{2} \rfloor$ and $Q := q^{m(m-1)/2n}$. Let Y be a subset of A_m that contains the zero form, and suppose that Y is a t-design for some t satisfying $0 \leq t < n$. Let $b = (b_0, b_1, \ldots, b_m)$ be the rank or the distance distribution of Y, and suppose that*

$$b_{2i} = 0 \quad \text{for } i = 1, 2, \ldots, n - t - 1. \tag{10}$$

Then

$$b_{2n-2i} = \begin{bmatrix} n \\ i \end{bmatrix} \sum_{j=i}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n-i \\ n-j \end{bmatrix} \left(\frac{|Y|}{Q^j} - 1 \right) \quad \text{for } i = 0, 1, \ldots, n-1.$$

Proof. First suppose that b is the distance distribution of Y, and let $(b'_0, b'_1, \ldots, b'_n)$ be the dual distance distribution of Y defined in (5). Then by the definition of a t-design

$$b'_k = 0 \quad \text{for } k = 1, 2, \ldots, t. \tag{11}$$

Using (3), we obtain

$$\sum_{k=0}^{j} \begin{bmatrix} n-k \\ n-j \end{bmatrix} b'_k = Q^j \sum_{i=0}^{n} b_{2i} \begin{bmatrix} n-i \\ j \end{bmatrix} \quad \text{for } j = 0, 1, \ldots, n,$$

and from (10), (11), and $b'_0 = |Y|$ by (6), we then deduce

$$\begin{bmatrix} n \\ j \end{bmatrix} \left(\frac{|Y|}{Q^j} - 1 \right) = \sum_{i=0}^{t} \begin{bmatrix} i \\ j \end{bmatrix} b_{2n-2i} \quad \text{for } j = 0, 1, \ldots, t.$$

By the inversion formula for p-binomial coefficients (see [DG75, Eq. (10)], for example), this is equivalent to the claim of the theorem.

Now suppose that b is the rank distribution of Y, and let $(b'_0, b'_1, \ldots, b'_n)$ be the dual rank distribution of Y defined in (4). Then by Lemma 1, (11) holds again, and the conclusion of the theorem remains true if b is the rank distribution of Y. □

The special case of Theorem 9, where b is the distance distribution of an alternating $(m, 2n-2t)$-set Y whose size meets the bound in Theorem 6, was proved in [DG75, Thm. 4 (ii)]. We can recover [DG75, Thm. 4 (ii)] from Theorem 9 since, if b is the distance distribution of Y, the condition (10) is satisfied for every $(m, 2n-2t)$-set Y and, by Theorem 6, an alternating $(m, 2n-2t)$-set of maximum size is automatically a $(t+1)$-design. Moreover, it follows from a general theorem on metric association schemes (see [DL98, Thm. 11], for example) that, if Y is an alternating $(m, 2n-2t)$-set and a t-design, then Y is distance invariant. Therefore, if the condition (10) is satisfied for b being the distance distribution of Y, then it is satisfied for b being the rank distribution of Y.

The new contribution of Theorem 9 is therefore twofold. Firstly, the theorem allows us to compute the rank or the distance distribution of an alternating (m, d)-set that has not necessarily maximum size. This situation occurs for example in Section 4, where we are interested in the rank distribution of alternating subsets of (m, d)-sets. (We note in passing that the alternating subset of an (m, d)-set of maximum size does not necessarily have maximum size as well.) Secondly, and more importantly, the theorem enables us to compute the rank distribution of a (non-additive) alternating (m, d)-set for which the distance distribution does not necessarily satisfy the condition (10). This fact will be crucially required in the proof of the following theorem.

Theorem 10. *Let $m > 1$ be an integer, write $n := \lfloor \frac{m}{2} \rfloor$, and let t be an integer satisfying $0 \le t \le n$. Let Y be an additive $(m, m-2t)$-set, and suppose that $\phi(Y)$ is a t-design. Let Y have rank distribution $(a_0, a_1, \ldots, a_m)$. Then, if m is odd,*

$$a_{m-2i} = \begin{bmatrix} n \\ i \end{bmatrix} \sum_{j=i}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n+1-i \\ n+1-j \end{bmatrix} \left(\frac{|Y|}{q^{jm}} - 1 \right) \qquad \text{for } i = 0, 1, \ldots, \tfrac{m-1}{2} \tag{12}$$

$$a_{m-2i+1} = p^{n-i+1} \begin{bmatrix} n \\ i-1 \end{bmatrix} \sum_{j=i}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n+1-i \\ n+1-j \end{bmatrix} \left(\frac{|Y|}{q^{jm}} - 1 \right) \quad \text{for } i = 1, 2, \ldots, \tfrac{m-1}{2}, \tag{13}$$

and if m is even,

$$a_{m-2i} = \begin{bmatrix} n \\ i \end{bmatrix} \sum_{j=i}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n-i \\ n-j \end{bmatrix} \left(\frac{|Y|}{q^{(m-1)j+2i}} - 1 \right) \qquad \text{for } i = 0, 1, \ldots, \tfrac{m-2}{2} \tag{14}$$

$$a_{m-2i+1} = (p^{n-i+1} - 1) \begin{bmatrix} n \\ i-1 \end{bmatrix} \sum_{j=i}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n-i \\ n-j \end{bmatrix} \frac{|Y|}{q^{(m-1)j+2i}} \quad \text{for } i = 1, 2, \ldots, \tfrac{m}{2}. \tag{15}$$

Proof. First note that the elements in $\psi(Y)$ are obtained by restricting the elements in $\phi(Y)$ onto an m-dimensional subspace. Thus, since $\phi(Y)$ is a t-design by assumption, $\psi(Y)$ is also a t-design by Theorem 3. Notice further that, for even m and $t = n$, we have $\phi(Y) = A_{m+1}$ by Theorem 3, which implies $\psi(Y) = A_m$. For odd m and $t = n$, we also have $\psi(Y) = A_m$ by Theorem 3.

Now write $r := |Y|/|\psi(Y)|$. Then, for $t < n$, we have $a_1 = 0$ and therefore $r = 1$ using Lemma 4 and the additive property of Y. If $t = n$, then $\psi(Y) = A_m$ and furthermore, since $\phi(Y)$ is an n-design, Theorem 3 implies that each element in A_m has r preimages in Y under ψ. Therefore, letting $(b_0, b_1, \ldots, b_{m+1})$ and $(c_0, c_1, \ldots, c_m)$ be the rank distributions of $\phi(Y)$ and $\psi(Y)$, respectively, application of Lemma 4 gives

$$\begin{aligned} a_{2i} + a_{2i-1} &= b_{2i} \quad \text{for } i = 0, 1, \ldots, n' \\ a_{2i} + a_{2i+1} &= r\, c_{2i} \quad \text{for } i = 0, 1, \ldots, n, \end{aligned} \tag{16}$$

where $n' := \lfloor \frac{m+1}{2} \rfloor$ and, by convention, $a_{-1} = a_{m+1} = 0$. Solving this system for $(a_0, a_1, \ldots, a_m)$, we obtain for odd m

$$a_{m-2i} = \sum_{k=0}^{i} b_{2n'-2k} - \sum_{k=0}^{i-1} r\, c_{2n-2k} \quad \text{for } i = 0, 1, \ldots, n'-1 \tag{17}$$

$$a_{m-2i+1} = \sum_{k=0}^{i-1} r\, c_{2n-2k} - \sum_{k=0}^{i-1} b_{2n'-2k} \quad \text{for } i = 1, 2, \ldots, n, \tag{18}$$

and for even m

$$a_{m-2i} = \sum_{k=0}^{i} r\, c_{2n-2k} - \sum_{k=0}^{i-1} b_{2n'-2k} \quad \text{for } i = 0, 1, \ldots, n'-1 \tag{19}$$

$$a_{m-2i+1} = \sum_{k=0}^{i-1} b_{2n'-2k} - \sum_{k=0}^{i-1} r\, c_{2n-2k} \quad \text{for } i = 1, 2, \ldots, n. \tag{20}$$

Next we compute the sums involved in the above equations. Since Y is an additive $(m, m-2t)$-set, we have

$$a_i = 0 \quad \text{for } i = 1, 2, \ldots, m-2t-1. \tag{21}$$

By assumption $\phi(Y)$ is a t-design, and by (21) and Lemma 4 we have $b_{2i} = 0$ for $i = 1, 2, \ldots, n'-t-1$. We can therefore apply Theorem 9 to $\phi(Y)$ to give

$$b_{2n'-2k} = \begin{bmatrix} n' \\ k \end{bmatrix} \sum_{j=k}^{t} (-1)^{j-k} p^{\binom{j-k}{2}} \begin{bmatrix} n'-k \\ n'-j \end{bmatrix} \left(\frac{|Y|}{(Q')^j} - 1 \right) \quad \text{for } k = 0, 1, \ldots, n'-1, \tag{22}$$

using $|\phi(Y)| = |Y|$ and writing $Q' := q^{m(m+1)/2n'}$. If $t < n'$, then (22) is a direct consequence of Theorem 9, while for $t = n'$, we first apply Theorem 9 with $t := n' - 1$ and then change the upper summation limit to n' since in this case $|\phi(Y)| = |A_{m+1}| = (Q')^n$. Similarly, since $\psi(Y)$ is a t-design and by (21) and Lemma 4 we have $c_{2i} = 0$ for $i = 1, 2, \ldots, n - t - 1$, Theorem 9 gives

$$r\, c_{2n-2k} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t} (-1)^{j-k} p^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} \left(\frac{|Y|}{Q^j} - r \right) \quad \text{for } k = 0, 1, \ldots, n-1, \tag{23}$$

using $r\,|\psi(Y)| = |Y|$ and writing $Q := q^{m(m-1)/2n}$. For $t = n$, we can use Newton's identity for p-binomial coefficients (see [DG75, Eq. (8)], for example) to show that the right-hand side of (23) is independent of r. Therefore, since $r = 1$ for $t < n$, we can rewrite (23) as

$$r\, c_{2n-2k} = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{j=k}^{t} (-1)^{j-k} p^{\binom{j-k}{2}} \begin{bmatrix} n-k \\ n-j \end{bmatrix} \left(\frac{|Y|}{Q^j} - 1 \right) \quad \text{for } k = 0, 1, \ldots, n-1. \tag{24}$$

Now, by applying elementary manipulations, we find from (22) that

$$\sum_{k=0}^{i} b_{2n'-2k} = \sum_{j=0}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n' \\ j \end{bmatrix} \begin{bmatrix} j-1 \\ i \end{bmatrix} \left(\frac{|Y|}{(Q')^j} - 1 \right) \quad \text{for } i = 0, 1, \ldots, n'-1, \tag{25}$$

where we have used the identity

$$\sum_{k=0}^{i} (-1)^k p^{\binom{j-k}{2}} \begin{bmatrix} j \\ k \end{bmatrix} = (-1)^i p^{\binom{j-i}{2}} \begin{bmatrix} j-1 \\ i \end{bmatrix},$$

which is easily proved by induction on i. A similar calculation applied to (24) gives

$$\sum_{k=0}^{i} r\, c_{2n-2k} = \sum_{j=0}^{t} (-1)^{j-i} p^{\binom{j-i}{2}} \begin{bmatrix} n \\ j \end{bmatrix} \begin{bmatrix} j-1 \\ i \end{bmatrix} \left(\frac{|Y|}{Q^j} - 1 \right) \quad \text{for } i = 0, 1, \ldots, n-1, \tag{26}$$

and the claimed result follows by substituting (25) and (26) into (17), (18), (19), and (20) and applying elementary manipulations. We omit the details. □

The theorem also gives the rank distribution of an additive $(m, m-2t+1)$-set Y provided that $\phi(Y)$ is a t-design. However, as shown below, this works only when m is even.

Remark 11. For odd m, Theorem 10 precludes the existence of an additive "true" $(m, m-2t+1)$-set Y such that $\phi(Y)$ is a t-design. To see this, suppose for a contradiction that Y is an additive $(m, m-2t+1)$-set, but not an $(m, m-2t+2)$-set, and that $\phi(Y)$ is a t-design. By assumption, we have $a_{m-2t} = 0$, forcing $|Y| = q^{tm}$ by (12). But then (13) gives $a_{m-2t+1} = 0$, so that Y is in fact an $(m, m-2t+2)$-set. This yields the desired contradiction.

As in Theorem 10, write $n := \lfloor \frac{m}{2} \rfloor$ for $m > 1$. If Y is an $(m, 2n-2t+1)$-set whose size meets the bound in Corollary 7, then $\phi(Y)$ is an alternating $(m+1, 2(n-t+1))$-set whose size meets the bound in Theorem 6. Hence, by Theorem 6, $\phi(Y)$ is a $(t+1)$-design for odd m and $\phi(Y)$ is a t-design for even m. Therefore, Theorem 10 certainly gives the rank distribution of additive (m, d)-sets of maximum size for odd d.

4 Constructions of (m, d)-Sets

In this section we provide constructions of (m, d)-sets for all possible values of m and d. It should be noted that, if Y is an alternating $(m+1, 2e)$-set whose size meets the bound in Theorem 6, then $\phi^{-1}(Y)$ is an $(m, 2e-1)$-set whose size meets the bound in Corollary 7. Therefore, when d is odd, an (m, d)-set of maximum size can be obtained from the results in [DG75]. However, we prefer to work directly in S_m, thereby getting unified constructions for odd and even d. Indeed, for odd m and odd d, we obtain an alternative description of the construction given in [DG75], while for even m and odd d, we could not decide whether our construction differs from that in [DG75].

Throughout this section we shall make use of the *trace function* $\mathrm{Tr}_m : \mathrm{GF}(q^m) \to \mathrm{GF}(q)$, which is defined by

$$\mathrm{Tr}_m(x) := \sum_{j=0}^{m-1} x^{q^j}.$$

It is easy to check that the trace function satisfies $\mathrm{Tr}_m(x^q) = \mathrm{Tr}_m(x)$ and acts linearly, that is, $\mathrm{Tr}_m(ax + by) = a\,\mathrm{Tr}_m(x) + b\,\mathrm{Tr}_m(y)$ for $a, b \in \mathrm{GF}(q)$. Another useful property is that the mapping $(x, y) \mapsto \mathrm{Tr}_m(xy)$ is an inner product on $\mathrm{GF}(q^m)$, as a vector space over $\mathrm{GF}(q)$.

4.1 The Case When $m - d$ is Even

In what follows, we take $V = \mathrm{GF}(q^m)$. Let t be an integer satisfying $0 \le t \le \frac{m-1}{2}$, and let $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_t) \in V^{t+1}$. Let $B_\lambda : V \times V \to K$ be given by

$$B_\lambda(x, y) := \mathrm{Tr}_m(\lambda_0 xy) + \sum_{j=1}^{t} \mathrm{Tr}_m(\lambda_j [x^{q^j} y + x y^{q^j}]). \tag{27}$$

It is readily verified that B_λ is a symmetric bilinear form. We define the subset Y of S_m by

$$Y := \{B_\lambda : \lambda \in V^{t+1}\}.$$

By the linearity of the trace function, Y is an additive set.

We show in Theorem 12 below that Y is an $(m, m-2t)$-set of size $q^{m(t+1)}$. We note that, when m is odd, the size of Y meets the upper bound in Corollary 7. In particular, for $t = \frac{m-1}{2}$ (hence, m is odd), we have $Y = S_m$. By Remark 8, Y has also maximum size for even m and $t = 0$. We will then use the combinatorial property of a t-design, given in Theorem 3, to show in Theorems 14 and 15 that $\theta(Y)$ (the alternating subset of Y) and $\phi(Y)$ are t-designs. Therefore, Theorem 10 gives the rank distribution of Y and Theorem 9 gives the rank distribution of $\theta(Y)$.

Before we prove these properties of Y, we include a discussion on the relation of Y to the results of [DG75] and comment on connections of this relation to the celebrated $\mathbb{Z}_4$-linearity [HKC+94] of the Kerdock code. In particular we show that, for m odd, $\phi(Y)$ is identical to the original (non-additive) alternating $(m+1, m+1-2t)$-set constructed in [DG75, Thm. 9], and therefore, we give an alternative description of this construction. Since K has even characteristic, we have

$$\sqrt{\mathrm{Tr}_m(x^2)} = \mathrm{Tr}_m(x), \tag{28}$$

and therefore,

$$\sqrt{B_\lambda(x, x)} = \mathrm{Tr}_m(\lambda_0' x),$$

where $\lambda_0' = \sqrt{\lambda_0}$. We then conclude from the definition (7) of ϕ that

$$\phi(B_\lambda)\big((x,\alpha),(y,\beta)\big) = \mathrm{Tr}_m\left((\lambda_0')^2 xy + \lambda_0' y\,\mathrm{Tr}_m(\lambda_0' x) + \lambda_0'(\beta x + \alpha y) + \sum_{j=1}^{t} \lambda_j [x^{q^j} y + x y^{q^j}]\right),$$

where we have used the linearity of the trace function. By comparing $\phi(B_\lambda)$ with the last displayed equation on [DG75, page 43], we conclude that for m odd, $\phi(Y)$ is identical to the alternating $(m+1, m+1-2t)$-set constructed in [DG75, Thm. 9].

For $q = 2$ and $t = 0$, the equivalence between $\phi(Y)$ and the construction in [DG75] for odd m was established in [CCKS97] by giving a new viewpoint on the $\mathbb{Z}_4$-linearity of the Kerdock code. In this case, $\phi(Y)$ gives rise to the $\mathbb{Z}_2$-Kerdock code $\mathcal{K}_2(m+1)$ (see [MS77, Ch. 15], for example), and it was shown in [CCKS97, Ex. 9.2] that Y itself can be used to construct the $\mathbb{Z}_4$-Kerdock code $\mathcal{K}_4(m)$, as defined in [HKC$^+$94]. A landmark result established in [HKC$^+$94] states that $\mathcal{K}_2(m+1)$ is obtained from $\mathcal{K}_4(m)$ via the *Gray map*, and a main result of [CCKS97] is that this transition is in fact induced by the mapping ϕ. We refer to [CCKS97, § 8] for a detailed discussion of this fact and to [GMR07] for a treatment of the more general case where q is a power of 2. We finally point out that, in analogy with [CCKS97, Ex. 9.2], we may also use the $(m, m-2t)$-set Y for $t > 0$ and odd m to construct the $\mathbb{Z}_4$-Delsarte–Goethals code, as defined in [HKC$^+$94].

In the remainder of this subsection, we prove the announced properties of Y.

Theorem 12. *Y is an $(m, m-2t)$-set of size $q^{m(t+1)}$.*

Proof. Since Y is an additive set, it is sufficient to show that, if λ is nonzero, then B_λ has rank at least $m-2t$. Pick a nonzero $\lambda \in V^{t+1}$, and note that we can write (27) as

$$B_\lambda(x,y) = \mathrm{Tr}_m(y L_\lambda(x)),$$

where

$$L_\lambda(x) = \lambda_0 x + \sum_{j=1}^{t} (\lambda_j x^{q^j} + (\lambda_j x)^{q^{-j}}).$$

Observe that $B_\lambda(x,y) = 0$ for each $y \in V$ if and only if $L_\lambda(x) = 0$. Since $x \mapsto x^{q^t}$ is an automorphism on V and $L_\lambda(x^{q^t})$ has algebraic degree at most q^{2t}, $L_\lambda(x)$ has at most q^{2t} roots in V. Therefore,

$$\dim_K(\mathrm{rad}(B_\lambda)) \le 2t,$$

so that B_λ has rank at least $m-2t$, as required. □

In order to show that $\phi(Y)$ and $\theta(Y)$ are t-designs, we prove the following lemma.

Lemma 13. *Let U be a k-dimensional subspace of V, and let ℓ be an arbitrary, but fixed, integer. Then every bilinear form $B : U \times V \to K$ can be expressed in the form*

$$B(x,y) = \sum_{j=0}^{k-1} \mathrm{Tr}_m(a_j y x^{q^{j-\ell}})$$

for some uniquely determined $a_0, a_1, \ldots, a_{k-1} \in V$.

Proof. The multiset containing the bilinear forms in the lemma has size q^{mk} and is closed under addition. It therefore remains to show that, if $B(x, y)$ is identically zero, then $a_0 = a_1 = \cdots = a_{k-1} = 0$. We may write

$$B(x, y) = \mathrm{Tr}_m(yL(x)), \quad \text{where} \quad L(x) = \sum_{j=0}^{k-1} a_j x^{q^{j-\ell}}.$$

If $B(x, y)$ is identically zero, then $L(x) = 0$ for all $x \in U$. Observe that $L(x^{q^\ell})$ has algebraic degree at most q^{k-1}. Hence, if the a_j's are not all zero, then $L(x)$ has at most q^{k-1} roots in V. The lemma follows since U is a subset of V containing q^k elements. □

Theorem 14. *$\theta(Y)$ is a t-design.*

Proof. It is not hard to verify that $B_\lambda \in \theta(Y)$ if and only if $\lambda_0 = 0$, so that all $B_\lambda \in \theta(Y)$ can be written as

$$B_\lambda(x, y) = \sum_{j=1}^{t} \mathrm{Tr}_m(\lambda_j[x^{q^j} y + x y^{q^j}]). \tag{29}$$

Let U be a $(2t + 1)$-dimensional subspace of V. In view of Theorem 3, we wish to show that the multiset

$$\{B|_{U\times U} : B \in \theta(Y)\} \tag{30}$$

contains each alternating bilinear form on U equally often.

Let $\mu = (\mu_0, \mu_1, \ldots, \mu_{2t}) \in V^{2t+1}$, and consider the bilinear form $D_\mu : V \times V \to K$ given by

$$D_\mu(x, y) = \sum_{j=0}^{2t} \mathrm{Tr}_m(\mu_j y x^{q^{j-t}}). \tag{31}$$

By applying Lemma 13 with $k = 2t + 1$ and $\ell = t$, we conclude that $\{D_\mu|_{U\times V} : \mu \in V^{2t+1}\}$ is the set of all bilinear mappings from $U \times V$ to K, and therefore, the multiset $\{D_\mu|_{U\times U} : \mu \in V^{2t+1}\}$ contains each bilinear mapping from $U \times U$ to K equally often. Now define the alternating bilinear form $C_\mu : V \times V \to K$ by

$$C_\mu(x, y) = D_\mu(x, y) + D_\mu(y, x). \tag{32}$$

Then the multiset $\{C_\mu|_{U\times U} : \mu \in V^{2t+1}\}$ contains each alternating bilinear form on U equally often. Substitution of (31) into (32) gives

$$\begin{aligned}
C_\mu(x, y) &= \sum_{j=0}^{2t} \mathrm{Tr}_m(\mu_j y x^{q^{j-t}} + \mu_j y^{q^{j-t}} x) \\
&= \sum_{j=0}^{t-1} \mathrm{Tr}_m(\mu_j y x^{q^{j-t}} + \mu_j y^{q^{j-t}} x) + \sum_{j=t+1}^{2t} \mathrm{Tr}_m(\mu_j y x^{q^{j-t}} + \mu_j y^{q^{j-t}} x) \\
&= \sum_{j=1}^{t} \mathrm{Tr}_m(\mu_{t-j} y x^{q^{-j}} + \mu_{t-j} y^{q^{-j}} x) + \sum_{j=1}^{t} \mathrm{Tr}_m(\mu_{t+j} y x^{q^j} + \mu_{t+j} y^{q^j} x) \\
&= \sum_{j=1}^{t} \mathrm{Tr}_m(\sigma_j[x^{q^j} y + x y^{q^j}]),
\end{aligned} \tag{33}$$

where

$$\sigma_j = \mu_{t+j} + \mu_{t-j}^{q^j} \quad \text{for } j = 1, 2, \ldots, t.$$

When μ runs through V^{2t+1}, the t-tuple $(\sigma_1, \sigma_2, \ldots, \sigma_t)$ ranges over V^t, where each t-tuple occurs q^{t+1} times. Then, by comparing (29) and (33), we conclude that the multiset (30) contains each alternating bilinear form on U an equal number of times. This completes the proof. □

Theorem 15. *$\phi(Y)$ is a t-design.*

Proof. From the definition of Y it is seen that Y is a union of q^m cosets of $\theta(Y)$ with coset representatives R_μ, where $\mu \in V$ and $R_\mu : V \times V \to K$ is given by

$$R_\mu(x, y) = \mathrm{Tr}_m(\mu xy). \tag{34}$$

Note that we have $\psi(B+C) = \psi(B)+C$ for each $B \in S_m$ and each $C \in A_m$. Hence, $\psi(Y)$ is a union of q^m cosets of $\theta(Y)$ with coset representatives $\psi(R_\mu)$. For each $\mu \in V$, the coset $\psi(R_\mu) + \theta(Y)$ has the same distance distribution as $\theta(Y)$. Therefore, since $\theta(Y)$ is a t-design by Theorem 14, each coset $\psi(R_\mu) + \theta(Y)$ is also a t-design. Now let U be a $(2t+1)$-dimensional subspace of V. Theorem 3 asserts that, for each $\mu \in V$, the multiset

$$\{\psi(R_\mu + B)|_{U\times U} : B \in \theta(Y)\} \tag{35}$$

contains each alternating bilinear form on U equally often.

We also have $\phi(B+C) = \phi(B)+\phi(C)$ for each $B \in S_m$ and each $C \in A_m$. It follows that $\phi(Y)$ is a union of q^m cosets of $\phi(\theta(Y))$ with coset representatives $\phi(R_\mu)$, given by

$$\phi(R_\mu)\big((x,\alpha),(y,\beta)\big) = \psi(R_\mu)(x,y) + \beta\sqrt{R_\mu(x,x)} + \alpha\sqrt{R_\mu(y,y)}.$$

From (28) and (34) we conclude $\sqrt{R_\mu(x,x)} = \mathrm{Tr}_m(\sqrt{\mu}x)$, and hence, when μ ranges over V, then $\sqrt{R_\mu(x,x)}$ ranges over all linear mappings from V to K. Using the properties of (35), we then conclude that the multiset

$$\{\phi(R_\mu + B)|_{(U\times K)\times(U\times K)} : B \in \theta(Y) \wedge \mu \in V\} = \{\phi(B)|_{(U\times K)\times(U\times K)} : B \in Y\}$$

contains every alternating bilinear form on the $(2t+2)$-dimensional subspace $U \times K$ of $V \times K$ an equal number of times. In view of Theorem 3, this completes the proof. □

4.2 The Case When $m - d$ is Odd

In what follows, let $V' = \mathrm{GF}(q^{m+1})$. We define V to be the m-dimensional subspace of V' given by the decomposition $V' = V \oplus K$, where $V \oplus K$ is the direct sum of V and K.

Let t be an integer satisfying $1 \le t \le \frac{m}{2}$. Write $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_t) \in (V')^t$, and define $B_\lambda : V \times V \to K$ to be the mapping

$$B_\lambda(x, y) := \sum_{j=1}^{t} \mathrm{Tr}_{m+1}(\lambda_j(x^{q^j} - x)(y^{q^j} - y)). \tag{36}$$

It is straightforward to show that B_λ is a symmetric bilinear form. We define the subset Y of S_m by

$$Y := \{B_\lambda : \lambda \in (V')^t\}.$$

By the linearity of the trace function, Y is an additive set. We will show in Theorem 16 that Y is an $(m, m-2t+1)$-set of size $q^{(m+1)t}$. Note that, when m is even, the size of Y meets the upper bound in Corollary 7. In particular, for $t = \frac{m}{2}$, we have $Y = S_m$.

When m is even, we will also show in Corollary 17 that $\phi(Y)$ is a t-design and in Theorem 18 that $\theta(Y)$ is a $(t-1)$-design. Therefore, for even m, the rank distribution of Y is given by Theorem 10 and the rank distribution of the alternating subset $\theta(Y)$ is given by Theorem 9. By Remark 11, $\phi(Y)$ is not a t-design for odd m (if it were, then Y would be an $(m, m-2t+2)$-set of size $q^{(m+1)t}$, which contradicts the bound $|Y| \leq q^{mt}$ in Corollary 7). Hence, for odd m, we cannot deduce the rank distribution of Y from the results of the previous section.

Theorem 16. *Y is an $(m, m-2t+1)$-set of size $q^{(m+1)t}$.*

Proof. Since Y is an additive set, it is sufficient to show that, if λ is nonzero, then B_λ has rank at least $m-2t+1$. Pick a nonzero $\lambda \in (V')^t$, and write (36) as

$$B_\lambda(x, y) = \mathrm{Tr}_{m+1}(yL_\lambda(x)),$$

where

$$L_\lambda(x) = \sum_{j=1}^{t} \Big[\lambda_j(x - x^{q^j}) + \lambda_j^{q^{-j}}(x - x^{q^{-j}})\Big].$$

Since $x \mapsto x^{q^t}$ is an automorphism on V' and $L_\lambda(x^{q^t})$ has algebraic degree at most q^{2t}, we conclude that $L_\lambda(x) = 0$ has at most q^{2t} solutions in V'. Since $L_\lambda(x)$ is a linearised polynomial, we can write $L_\lambda(x+a) = L_\lambda(x) + L_\lambda(a)$ for all $x, a \in V'$. But, for each $a \in K$, we have $L_\lambda(a) = 0$, which implies that, if $L_\lambda(x) = 0$, then $L_\lambda(x+a) = 0$. For each $x \in V$ and each $a \in K$, we have $(x+a) \notin V$, so the number of $x \in V$ such that $L_\lambda(x) = 0$ is at most q^{2t-1}. Since $B_\lambda(x, y) = 0$ for each $y \in V$ occurs only if $L_\lambda(x) = 0$, we conclude that

$$\dim_K(\mathrm{rad}(B_\lambda)) \leq 2t-1.$$

Hence, the rank of B_λ is at least $m-2t+1$, as required. □

When m is even, $\phi(Y)$ is an $(m+1, m-2t+2)$-set whose size meets the bound in Theorem 6, and hence Theorem 6 gives the following.

Corollary 17. *When m is even, $\phi(Y)$ is a t-design.*

We now use this result to show that $\theta(Y)$ is a $(t-1)$-design.

Theorem 18. *When m is even, $\theta(Y)$ is a $(t-1)$-design.*

Proof. Let m be even, and let U be a $(2t)$-dimensional subspace of V, so that $U \times K$ is a $(2t+1)$-dimensional subspace of $V \times K$. By Corollary 17, $\phi(Y)$ is a t-design, and hence by Theorem 3, the multiset

$$\{\phi(B)|_{(U\times K)\times(U\times K)} : B \in Y\}$$

contains each alternating bilinear form on $U \times K$ equally often. But for each $B \in Y$ we have

$$\phi(B)\big((x,\alpha),(y,\beta)\big) = B(x,y) \quad \text{if and only if } B \in \theta(Y).$$

Therefore, denoting by $O = \{0\}$ the trivial subspace of K, it follows that the multiset

$$\{\phi(B)|_{(U\times O)\times(U\times O)} : B \in \theta(Y)\} = \{B|_{U\times U} : B \in \theta(Y)\}$$

contains each alternating bilinear form on U equally often. In view of Theorem 3, this completes the proof. □

5 Final Remarks

We have already noted that our constructions of (m, d)-sets are optimal (that is, they have largest possible size) when d is odd and when $d = m$. It is an open question whether our constructions are also optimal when d is even and $d < m$. We found it difficult to improve the bound on the size of an (m, d)-set, given in Corollary 7, and leave such an improvement as an open problem.

We have constrained our study to fields of even characteristic, mainly because the mappings ϕ and ψ are only defined when the characteristic of K is even. Some results, however, hold also for fields of odd characteristic. It is a consequence of Proposition 19, stated below, that Corollary 7 is valid for all finite K. Moreover, our constructions work for all finite K, as the proofs of Theorems 12 and 16 do not require that K has even characteristic.

Finally, we comment on a connection between the association scheme of alternating bilinear forms (A_{m+1}, R), as defined in Section 2.2, and an association scheme defined on S_m. Suppose that the characteristic of K is arbitrary (but nonzero). Write $n := \lfloor \frac{m+1}{2} \rfloor$. Define the relations

$$R'_i = \{(B, C) \in S_m \times S_m : \operatorname{rank}(B - C) = 2i \text{ or } 2i - 1\} \quad \text{for } i = 0, 1, \ldots, n,$$

and write $R' = (R'_0, R'_1, \ldots, R'_n)$.

Proposition 19. *The association schemes (S_m, R') and (A_{m+1}, R) have the same intersection numbers (and consequently the same eigenvalues).*

Proof. If the characteristic of K is odd, the theorem was proved by Egawa [Ega85, Thm. 2]. If the characteristic of K is even, the theorem is a consequence of (9) (or, alternatively, of the remarks at the end of [CCKS97, § 7]). □

References

[And76] G. E. Andrews. *The Theory of Partitions*, volume 2 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 1976.

[BCN89] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer-Verlag, Berlin Heidelberg, 1989.

[BI84] E. Bannai and T. Ito. *Algebraic Combinatorics I: Association Schemes*. Benjamin/Cummings, Menlo Park, California, 1984.

[Bro72] E. H. Brown, Jr. Generalizations of the Kervaire invariant. *Annals Math.*, 95(2):368–383, Mar. 1972.

[CCKS97] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. $\mathbb{Z}_4$-Kerdock codes, orthogonal spreads, and extremal Euclidean line sets. *Proc. London Math. Soc.*, 75(3):436–480, 1997.

[Del73] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, 10, 1973.

[Del78] P. Delsarte. Bilinear forms over a finite field with applications to coding theory. *J. Comb. Theory (A)*, 25(3):226–241, 1978.

[DG75] P. Delsarte and J. M. Goethals. Alternating bilinear forms over GF(q). *J. Comb. Theory (A)*, 19(1):26–50, 1975.

[DL98] P. Delsarte and V. I. Levenshtein. Association schemes and coding theory. *IEEE Trans. Inf. Theory*, 44(6):2477–2504, Oct. 1998.

[Ega85] Y. Egawa. Association schemes of quadratic forms. *J. Comb. Theory (A)*, 38(1):1–14, 1985.

[GMR07] S. González, C. Martínez, and I. F. Rúa. Symplectic spread-based generalized Kerdock codes. *Des. Codes Cryptogr.*, 42(2):213–226, Feb. 2007.

[HKC+94] A. Roger Hammons, Jr., P. Vijay Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals and related codes. *IEEE Trans. Inf. Theory*, 40(2):301–319, Mar. 1994.

[LDR07] M. C. López-Díaza and I. F. Rúa. An invariant for quadratic forms valued in Galois rings of characteristic 4. *Finite Fields Appl.*, 13(4):946–961, Nov. 2007.

[MS77] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.

[Mun86] A. Munemasa. An analogue of t-designs in the association schemes of alternating bilinear forms. *Graphs Comb.*, 2(1):259–267, Dec. 1986.

[Sch09] K.-U. Schmidt. $\mathbb{Z}_4$-valued quadratic forms and quaternary sequence families. *IEEE Trans. Inf. Theory*, 55(12):5803–5810, Dec. 2009.

[Sta86] D. Stanton. t-designs in classical association schemes. *Graphs Comb.*, 2(1):283–286, Dec. 1986.

[Woo93] J. A. Wood. Witt's extension theorem for mod four valued quadratic forms. *Trans. Amer. Math. Soc.*, 336(1):445–461, Mar. 1993.