

# Bent Vectorial Functions, Codes and Designs

Cunsheng Ding<sup>1</sup>, Akihiro Munemasa<sup>2</sup>, and Vladimir D. Tonchev

**Abstract**—Bent functions, or equivalently, Hadamard difference sets in the elementary Abelian group  $(\text{GF}(2^{2m}), +)$ , have been employed to construct symmetric and quasi-symmetric designs having the symmetric difference property. The main objective of this paper is to use bent vectorial functions for a construction of a two-parameter family of binary linear codes that do not satisfy the conditions of the Assmus–Mattson theorem, but nevertheless hold 2-designs. A new coding-theoretic characterization of bent vectorial functions is presented.

**Index Terms**—Bent function, bent vectorial function, linear code, 2-design.

## I. INTRODUCTION, MOTIVATIONS AND OBJECTIVES

WE START with a brief review of combinatorial  $t$ -designs (cf. [1], [3], [22]). Let  $\mathcal{P}$  be a set of  $v \geq 1$  elements, called *points*, and let  $\mathcal{B}$  be a collection of  $k$ -subsets of  $\mathcal{P}$ , called *blocks*, where  $k$  is a positive integer,  $1 \leq k \leq v$ . Let  $t$  be a non-negative integer,  $t \leq k$ . The pair  $\mathbb{D} = (\mathcal{P}, \mathcal{B})$  is called a  $t$ -( $v, k, \lambda$ ) *design*, or simply  $t$ -*design*, if every  $t$ -subset of  $\mathcal{P}$  is contained in exactly  $\lambda$  blocks of  $\mathcal{B}$ . We usually use  $b$  to denote the number of blocks in  $\mathcal{B}$ . A  $t$ -design is called *simple* if  $\mathcal{B}$  does not contain any repeated blocks. In this paper, we consider only simple  $t$ -designs.

Two designs are *isomorphic* if there is a bijection between their point sets that maps every block of the first design to a block of the second design. An *automorphism* of a design is any isomorphism of the design to itself. The set of all automorphisms of a design  $\mathbb{D}$  form the (full) automorphism group of  $\mathbb{D}$ .

It is clear that  $t$ -designs with  $k = t$  or  $k = v$  always exist. Such  $t$ -designs are called *trivial*. In this paper, we consider only  $t$ -designs with  $v > k > t$ .

The incidence matrix of a design  $\mathbb{D}$  is a  $(0, 1)$ -matrix  $A = (a_{ij})$  with rows labeled by the blocks, columns labeled by the points, where  $a_{i,j} = 1$  if the  $i$ th block contains the  $j$ th point, and  $a_{i,j} = 0$  otherwise. If the incidence matrix is viewed over  $\text{GF}(q)$ , its rows span a linear code of length  $v$  over

Manuscript received August 25, 2018; revised April 24, 2019; accepted May 5, 2019. Date of publication June 13, 2019; date of current version October 18, 2019. C. Ding was supported by the Hong Kong Research Grants Council under Grant 16300418. V. D. Tonchev was supported in part by the Fulbright Grant.

C. Ding is with the Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong (e-mail: cding@ust.hk).

A. Munemasa is with the Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan (e-mail: munemasa@math.is.tohoku.ac.jp).

V. D. Tonchev is with the Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931 USA (e-mail: tonchev@mtu.edu).

Communicated by C. Xing, Associate Editor for Coding Theory.

Digital Object Identifier 10.1109/TIT.2019.2922401

$\text{GF}(q)$ , which is denoted by  $\mathcal{C}_q(\mathbb{D})$  and is called the code of the design. Note that a  $t$ -design can be employed to construct linear codes in different ways. The supports of codewords of a given Hamming weight  $k$  in a code  $\mathcal{C}$  may form a  $t$ -design, which is referred to as a design supported by the code.

A design is called *symmetric* if  $v = b$ . A 2-( $v, k, \lambda$ ) design is symmetric if and only if every two blocks share exactly  $\lambda$  points.

A 2-design is *quasi-symmetric* with intersection numbers  $x$  and  $y$ , ( $x < y$ ) if any two blocks intersect in either  $x$  or  $y$  points.

Let  $\mathbb{D} = \{\mathcal{P}, \mathcal{B}\}$  be a 2-( $v, k, \lambda$ ) symmetric design, where  $\mathcal{B} = \{B_1, B_2, \dots, B_v\}$  and  $v \geq 2$ . Then

- $(B_1, \{B_2 \cap B_1, B_3 \cap B_1, \dots, B_v \cap B_1\})$  is a 2-( $k, \lambda, \lambda-1$ ) design, and called the *derived design* of  $\mathbb{D}$  with respect to  $B_1$ ;
- $(\overline{B}_1, \{B_2 \cap \overline{B}_1, B_3 \cap \overline{B}_1, \dots, B_v \cap \overline{B}_1\})$  is a 2-( $v-k, k-\lambda, \lambda$ ) design, called the *residual design* of  $\mathbb{D}$  with respect to  $B_1$ , where  $\overline{B}_1 = \mathcal{P} \setminus B_1$ .

If a symmetric design  $\mathbb{D}$  has parameters

$$2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}), \quad (1)$$

its derived designs have parameters

$$2 - (2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2} - 2^{m-1} - 1),$$

and its residual designs have parameters

$$2 - (2^{2m-1} + 2^{m-1}, 2^{2m-2}, 2^{2m-2} - 2^{m-1}).$$

A symmetric 2-design is said to have the *symmetric difference property*, or to be a *symmetric SDP design* (Kantor [14], [15]), if the symmetric difference of any *three* blocks is either a block or the complement of a block. Any derived or residual design of a symmetric SDP design is quasi-symmetric, and has the property that the symmetric difference of every two blocks is either a block or the complement of a block. The derived and residual designs of a symmetric SDP design are called quasi-symmetric SDP designs [12]. The binary codes of quasi-symmetric SDP designs give rise to an exponentially growing number of inequivalent linear codes that meet the Grey–Rankin bound [11]. It was proved in [21] that any quasi-symmetric SDP design can be embedded as a derived or a residual design in exactly one (up to isomorphism) symmetric SDP design.

A coding-theoretical characterization of symmetric SDP designs was given by Dillon and Schatz [8], who proved that any symmetric SDP design with parameters (1) is supported by the codewords of minimum weight in a binary linear code

$\mathcal{C}$  of length  $2^{2m}$ , dimension  $2m+2$  and weight enumerator given by

$$1 + 2^{2m}z^{2^{2m-1}-2^{m-1}} + (2^{2m+1}-2)z^{2^{2m-1}} + 2^{2m}z^{2^{2m-1}+2^{m-1}} + z^{2m}, \quad (2)$$

where  $\mathcal{C}$  is spanned by the first order Reed-Muller code  $\text{RM}_2(1, 2m)$  and a vector  $u$  being the truth table (introduced in Section III) of a bent function in  $2m$  variables, or equivalently,  $u$  is the incidence vector of a Hadamard difference set in the additive group of  $\text{GF}(2)^{2m}$  with parameters

$$(2^{2m}, 2^{2m-1} \pm 2^{m-1}, 2^{2m-2} \pm 2^{m-1}). \quad (3)$$

One of the objectives of this paper is to give a coding-theoretical characterization of bent vectorial functions (Theorem 5), which generalizes the Dillon and Schatz characterization of single bent functions [8]. Another objective is to present in Theorem 11 a two-parameter family of binary linear codes with parameters

$$[2^{2m}, 2m+1+\ell, 2^{2m-1}-2^{m-1}], \quad m \geq 2, \quad 1 \leq \ell \leq m,$$

that are based on bent vectorial functions and support 2-designs, despite that these codes do not satisfy the conditions of the Assmus-Mattson theorem (see Theorem 1). The subclass of codes with  $\ell = 1$  consists of codes introduced by Dillon and Schatz [8] that are based on bent functions and support symmetric SDP designs. Examples of codes with  $\ell = m$  are given that are optimal in the sense that they have the maximum possible minimum distance for the given length and dimension, or have the largest known minimum distance for the given length and dimension (see Note 6 in Section IV, and the examples thereafter).

## II. THE CLASSICAL CONSTRUCTIONS OF $t$ -DESIGNS FROM CODES

A simple sufficient condition for the supports of codewords of any given weight in a linear code to support a  $t$ -design is that the code admits a  $t$ -transitive or  $t$ -homogeneous automorphism group. All codes considered in this paper are of even length  $n$  of the form  $n = 2^{2m}$ . It is known that any 2-homogeneous group of even degree is necessarily 2-transitive (Kantor [13], [16]).

Another sufficient condition is given by the Assmus-Mattson theorem. Let  $\mathcal{C}$  be a  $[v, \kappa, d]$  linear code over  $\text{GF}(q)$ , and let  $A_i = A_i(\mathcal{C})$  be the number of codewords of Hamming weight  $i$  in  $\mathcal{C}$  ( $0 \leq i \leq v$ ). For each  $k$  with  $A_k \neq 0$ , let  $\mathcal{B}_k$  denote the set of the supports of all codewords of Hamming weight  $k$  in  $\mathcal{C}$ , where the code coordinates are indexed by  $1, 2, \dots, v$ . Let  $\mathcal{P} = \{1, 2, \dots, v\}$ . The following theorem, proved by Assmus and Mattson, provides sufficient conditions for the pair  $(\mathcal{P}, \mathcal{B}_k)$  to be a  $t$ -design.

**Theorem 1** (The Assmus-Mattson Theorem [2]). *Let  $\mathcal{C}$  be a binary  $[v, \kappa, d]$  code, and let  $d^\perp$  be the minimum weight of the dual code  $\mathcal{C}^\perp$ . Suppose that  $A_i = A_i(\mathcal{C})$  and  $A_i^\perp = A_i(\mathcal{C}^\perp)$ ,  $0 \leq i \leq v$ , are the weight distributions of  $\mathcal{C}$  and  $\mathcal{C}^\perp$ , respectively. Fix a positive integer  $t$  with  $t < d$ , and let  $s$  be*

*the number of  $i$  with  $A_i^\perp \neq 0$  for  $0 < i \leq v-t$ . If  $s \leq d-t$ , then*

- *the codewords of weight  $i$  in  $\mathcal{C}$  hold a  $t$ -design provided that  $A_i \neq 0$  and  $d \leq i \leq v$ , and*
- *the codewords of weight  $i$  in the code  $\mathcal{C}^\perp$  hold a  $t$ -design provided that  $A_i^\perp \neq 0$  and  $d^\perp \leq i \leq v-t$ .*

The parameter  $\lambda$  of a  $t$ -( $v, w, \lambda$ ) design supported by the codewords of weight  $w$  in a binary code  $\mathcal{C}$  is determined by

$$A_w = \lambda \binom{v}{t} / \binom{w}{t}.$$

## III. BENT FUNCTIONS AND BENT VECTORIAL FUNCTIONS

Let  $f = f(x)$  be a Boolean function from  $\text{GF}(2^n)$  to  $\text{GF}(2)$ . The support  $S_f$  of  $f$  is defined as

$$S_f = \{x \in \text{GF}(2^n) : f(x) = 1\} \subseteq \text{GF}(2^n).$$

The  $(0, 1)$  incidence vector of  $S_f$ , having its coordinates labeled by the elements of  $\text{GF}(2^n)$ , is called the *truth table* of  $f$ .

The *Walsh transform* of  $f$  is defined by

$$\hat{f}(w) = \sum_{x \in \text{GF}(2^n)} (-1)^{f(x) + \text{Tr}_{n/1}(wx)}$$

where  $w \in \text{GF}(2^n)$  and  $\text{Tr}_{n/n'}(x)$  denotes the trace function from  $\text{GF}(2^n)$  to  $\text{GF}(2^{n'})$ .

Two Boolean functions  $f$  and  $g$  from  $\text{GF}(2^n)$  to  $\text{GF}(2)$  are called *weakly affinely equivalent* or *EA-equivalent* if there are an automorphism  $A$  of  $(\text{GF}(2^n), +)$ , a homomorphism  $L$  from  $(\text{GF}(2^n), +)$  to  $(\text{GF}(2), +)$ , an element  $a \in \text{GF}(2^n)$  and an element  $b \in \text{GF}(2)$  such that

$$g(x) = f(A(x) + a) + L(x) + b$$

for all  $x \in \text{GF}(2^n)$ .

A Boolean function  $f$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)$  is called a *bent* function if  $|\hat{f}(w)| = 2^m$  for every  $w \in \text{GF}(2^{2m})$ . It is well known that a function  $f$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)$  is bent if and only if  $S_f$  is a difference set in  $(\text{GF}(2^{2m}), +)$  with parameters (3) [19].

A Boolean function  $f$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)$  is a bent function if and only if its truth table is at Hamming distance  $2^{2m-1} \pm 2^{m-1}$  from every codeword of the first order Read-Muller code  $\text{RM}_2(1, 2m)$  [18, Theorem 6, page 426]. It follows that

$$|S_f| = 2^{2m-1} \pm 2^{m-1}.$$

There are many constructions of bent functions. The reader is referred to [6] and [19] for detailed information about bent functions.

Let  $\ell$  be a positive integer, and let  $f_1(x), \dots, f_\ell(x)$  be Boolean functions from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)$ . The function  $F(x) = (f_1(x), \dots, f_\ell(x))$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^\ell$  is called a  $(2m, \ell)$  *vectorial Boolean function*.

A  $(2m, \ell)$  vectorial Boolean function  $F(x) = (f_1(x), \dots, f_\ell(x))$  is called a *bent vectorial function* if  $\sum_{j=1}^{\ell} a_j f_j(x)$  is a bent function for each nonzero  $(a_1, \dots, a_\ell) \in \text{GF}(2)^\ell$ .

For another equivalent definition of bent vectorial functions, see [7] or [19, Chapter 12].

Bent vectorial functions exist only when  $\ell \leq m$  (cf. [19, Chapter 12]). There are a number of known constructions of bent vectorial functions. The reader is referred to [7] and [19, Chapter 12] for detailed information. Below we present a specific construction of bent vectorial functions from [7].

**Example 2.** [7]. Let  $m \geq 1$  be an odd integer,  $\beta_1, \beta_2, \dots, \beta_m$  be a basis of  $\text{GF}(2^m)$  over  $\text{GF}(2)$ , and let  $u \in \text{GF}(2^{2m}) \setminus \text{GF}(2^m)$ . Let  $i$  be a positive integer with  $\gcd(2m, i) = 1$ . Then

$$\left( \text{Tr}_{2m/1}(\beta_1 ux^{2^i+1}), \text{Tr}_{2m/1}(\beta_2 ux^{2^i+1}), \dots, \text{Tr}_{2m/1}(\beta_m ux^{2^i+1}) \right)$$

is a  $(2m, m)$  bent vectorial function.

Under a basis of  $\text{GF}(2^\ell)$  over  $\text{GF}(2)$ ,  $(\text{GF}(2^\ell), +)$  and  $(\text{GF}(2)^\ell, +)$  are isomorphic. Hence, any vectorial function  $F(x) = (f_1(x), \dots, f_\ell(x))$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^\ell$  can be viewed as a function from  $\text{GF}(2^{2m})$  to  $\text{GF}(2^\ell)$ .

It is well known that a function  $F$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2^\ell)$  is bent if and only if  $\text{Tr}_{\ell/1}(aF(x))$  is a bent Boolean function for all  $a \in \text{GF}(2^\ell)^*$ . Any such vectorial function  $F$  can be expressed as  $\text{Tr}_{2m/\ell}(f(x))$ , where  $f$  is a univariate polynomial. This presentation of bent vectorial functions is more compact. We give two examples of bent vectorial functions in this form.

**Example 3.** (cf. [19, Chapter 12]). Let  $m > 1$  and  $i \geq 1$  be integers such that  $2m/\gcd(i, 2m)$  is even. Then  $\text{Tr}_{2m/m}(ax^{2^i+1})$  is bent if and only if  $\gcd(2^i+1, 2^m+1) \neq 1$  and  $a \in \text{GF}(2^{2m})^* \setminus \langle \alpha^{\gcd(2^i+1, 2^m+1)} \rangle$ , where  $\alpha$  is a generator of  $\text{GF}(2^{2m})^*$ .

**Example 4.** (cf. [19, Chapter 12]). Let  $m > 1$  and  $i \geq 1$  be integers such that  $\gcd(i, 2m) = 1$ . Let  $d = 2^{2i} - 2^i + 1$ . Let  $m$  be odd. Then  $\text{Tr}_{2m/m}(ax^d)$  is bent if and only if  $a \in \text{GF}(2^{2m})^* \setminus \langle \alpha^3 \rangle$ , where  $\alpha$  is a generator of  $\text{GF}(2^{2m})^*$ .

#### IV. A CONSTRUCTION OF CODES FROM BENT VECTORIAL FUNCTIONS

Let  $q = 2^{2m}$ , let  $\text{GF}(q) = \{u_1, u_2, \dots, u_q\}$ , and let  $w$  be a generator of  $\text{GF}(q)^*$ . For the purposes of what follows, it is convenient to use the following generator matrix of the binary  $[2^{2m}, 2m+1, 2^{2m-1}]$  first-order Reed-Muller code  $\text{RM}_2(1, 2m)$ :

$$G_0 = \begin{bmatrix} 1 & \dots & 1 \\ \text{Tr}_{2m/1}(w^0 u_1) & \dots & \text{Tr}_{2m/1}(w^0 u_q) \\ \vdots & \ddots & \vdots \\ \text{Tr}_{2m/1}(w^{2m-1} u_1) & \dots & \text{Tr}_{2m/1}(w^{2m-1} u_q) \end{bmatrix}.$$

The weight enumerator of  $\text{RM}_2(1, 2m)$  is

$$1 + (2^{2m+1} - 2)z^{2^{2m-1}} + z^{2^m}. \quad (4)$$

Two binary linear codes are equivalent if there is a permutation of coordinates that sends the first code to the second. Up to equivalence,  $\text{RM}_2(1, 2m)$  is the unique linear binary code with parameters  $[2^{2m}, 2m+1, 2^{2m-1}]$  [8]. Its dual code is the  $[2^{2m}, 2^{2m} - 1 - 2m, 4]$  Reed-Muller code of order  $2m - 2$ .

Both codes hold 3-designs since they are invariant under a 3-transitive affine group. Note that  $\text{RM}_2(1, 2m)^\perp$  is the unique, up to equivalence, binary linear code for the given parameters, hence it is equivalent to the extended binary linear Hamming code.

Let  $F(x) = (f_1(x), f_2(x), \dots, f_\ell(x))$  be a  $(2m, \ell)$  vectorial function from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^\ell$ . For each  $i$ ,  $1 \leq i \leq \ell$ , we define a binary vector

$$F_i = (f_i(u_1), f_i(u_2), \dots, f_i(u_q)) \in \text{GF}(2)^{2^{2m}},$$

which is the truth table of the Boolean function  $f_i(x)$  introduced in Section III.

Let  $\ell$  be an integer in the range  $1 \leq \ell \leq m$ . We now define a  $(2m+1+\ell) \times 2^{2m}$  matrix

$$G = G(f_1, \dots, f_\ell) = \begin{bmatrix} G_0 \\ F_1 \\ \vdots \\ F_\ell \end{bmatrix}, \quad (5)$$

where  $G_0$  is the generator matrix of  $\text{RM}_2(1, 2m)$ . Let  $\mathcal{C}(f_1, \dots, f_\ell)$  denote the binary code of length  $2^{2m}$  with generator matrix  $G(f_1, \dots, f_\ell)$  given by (5). The dimension of the code has the following lower and upper bounds:

$$2m+1 \leq \dim(\mathcal{C}(f_1, \dots, f_\ell)) \leq 2m+1+\ell.$$

The following theorem gives a coding-theoretical characterization of bent vectorial functions.

**Theorem 5.** A  $(2m, \ell)$  vectorial function  $F(x) = (f_1(x), f_2(x), \dots, f_\ell(x))$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^\ell$  is a bent vectorial function if and only if the code  $\mathcal{C}(f_1, \dots, f_\ell)$  with generator matrix  $G$  given by (5) has weight enumerator

$$1 + (2^\ell - 1)2^{2m}z^{2^{2m-1}-2^{m-1}} + 2(2^{2m} - 1)z^{2^{2m-1}} + (2^\ell - 1)2^{2m}z^{2^{2m-1}+2^{m-1}} + z^{2^m}. \quad (6)$$

*Proof.* By the definition of  $G$ , the code  $\mathcal{C}(f_1, \dots, f_\ell)$  contains the first-order Reed-Muller code  $\text{RM}_2(1, 2m)$  as a subcode, having weight enumerator (4).

It follows from (5) that every codeword of  $\mathcal{C}(f_1, \dots, f_\ell)$  must be the truth table of a Boolean function of the form

$$f_{(u,v,h)}(x) = \sum_{i=1}^{\ell} u_i f_i(x) + \sum_{j=0}^{2m-1} v_j \text{Tr}_{2m/1}(w^j x) + h,$$

where  $u_i, v_j, h \in \text{GF}(2)$ ,  $x \in \text{GF}(2^{2m})$ .

Suppose that  $F(x) = (f_1(x), f_2(x), \dots, f_\ell(x))$  is a  $(2m, \ell)$  bent vectorial function. When  $(u_1, \dots, u_\ell) = (0, \dots, 0)$ ,  $(v_0, v_1, \dots, v_{2m-1})$  runs over  $\text{GF}(2)^{2m}$  and  $h$  runs over  $\text{GF}(2)$ , the truth tables of the functions  $f_{(u,v,h)}(x)$  form the code  $\text{RM}_2(1, 2m)$ . Whenever  $(u_1, \dots, u_\ell) \neq (0, \dots, 0)$ , it follows from (5) that  $f_{(u,v,h)}(x)$  is a bent function, and the corresponding codeword has Hamming weight  $2^{2m-1} \pm 2^{m-1}$ . Since the all-one vector belongs to  $\text{RM}_2(1, 2m)$ , the code  $\mathcal{C}(f_1, \dots, f_\ell)$  is self-complementary, and the desired weight enumerator of  $\mathcal{C}(f_1, \dots, f_\ell)$  follows.

Suppose that  $\mathcal{C}(f_1, \dots, f_\ell)$  has weight enumerator given by (6). Then  $\mathcal{C}(f_1, \dots, f_\ell)$  has dimension  $2m+1+\ell$ . Consequently,  $\sum_{i=1}^{\ell} u_i f_i(x)$  is the zero function if and only if

$(u_1, \dots, u_\ell) = (0, \dots, 0)$ . It then follows that the codewords corresponding to  $f_{(u,v,h)}(x)$  must have Hamming weight  $2^{2m-1} \pm 2^{m-1}$  for all  $u = (u_1, \dots, u_\ell) \neq (0, \dots, 0)$  and all  $(v_0, v_1, \dots, v_{2m-1}) \in \text{GF}(2)^{2m}$ . Notice that

$$\sum_{j=0}^{2m-1} v_j \text{Tr}_{2m/1}(w^j x)$$

ranges over all linear functions from  $\text{GF}(2^m)$  to  $\text{GF}(2)$  when  $(v_0, v_1, \dots, v_{2m-1})$  runs over  $\text{GF}(2)^{2m}$ . Consequently,  $F(x)$  is a bent vectorial function.  $\square$

**Note 6.** Let  $F(x) = (f_1(x), f_2(x), \dots, f_m(x))$  be a bent vectorial function from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^m$ . Then the code  $\mathcal{C}(f_1, \dots, f_m)$  has parameters

$$[2^{2m}, 3m + 1, 2^{2m-1} - 2^{m-1}].$$

In particular, if  $m = 2$ , any code  $\mathcal{C}(f_1, f_2)$  based on a bent vectorial function from  $\text{GF}(2^4)$  to  $\text{GF}(2)^2$  has parameters  $[16, 7, 6]$  and is optimal (cf. [10]). An  $[n, k, d]$  code is optimal if  $d$  is the maximum possible minimum distance for the given  $n$  and  $k$ . If  $m = 3$ , any code  $\mathcal{C}(f_1, f_2, f_3)$  based on a bent vectorial function from  $\text{GF}(2^6)$  to  $\text{GF}(2)^3$  has parameters  $[64, 10, 28]$  and is optimal [10]. If  $m = 4$ , any code  $\mathcal{C}(f_1, \dots, f_4)$  based on a bent vectorial function from  $\text{GF}(2^8)$  to  $\text{GF}(2)^4$  has parameters  $[256, 13, 120]$  and has the largest known minimum distance for the given code length and dimension [10].

**Theorem 7.** *Up to equivalence, there is exactly one  $[16, 7, 6]$  code that can be obtained from a  $(4, 2)$  bent vectorial function.*

*Proof.* The weight enumerator of the second order Reed-Muller code  $\text{RM}_2(2, 4)$  is given by

$$1 + 140z^4 + 448z^6 + 870z^8 + 448z^{10} + 140z^{12} + z^{16}.$$

The truth table of a bent function  $f$  from  $\text{GF}(2^4)$  to  $\text{GF}(2)$  is a codeword  $c_f$  of  $\text{RM}_2(2, 4)$  of weight 6. The linear code  $\mathcal{C}(f)$  spanned by  $c_f$  and  $\text{RM}_2(1, 4)$  is a subcode of  $\text{RM}_2(2, 4)$  of dimension 6, having weight enumerator

$$1 + 16z^6 + 30z^8 + 16z^{10} + z^{16}.$$

The codewords of  $\mathcal{C}(f)$  of weight 6 form a symmetric 2-(16, 6, 2) SDP design, whose blocks correspond to the supports of 16 bent functions.

Now, let  $(f_1, f_2)$  be a  $(4, 2)$  bent vectorial function. Then, the intersection of the codes  $\mathcal{C}(f_1), \mathcal{C}(f_2)$  consists of the first order Reed-Muller code  $\text{RM}_2(1, 4)$ . It follows that the set of 448 codewords of weight 6 in  $\text{RM}_2(2, 4)$  is a union  $\mathcal{U}$  of 28 pairwise disjoint subsets of size 16, corresponding to the incidence matrices of symmetric 2-(16, 6, 2) SDP designs associated with 28 different  $[16, 6]$  codes defined by single bent functions.

If  $\mathcal{C}(f_1, f_2)$  is a  $[16, 7]$  code defined by a bent vectorial function  $(f_1, f_2)$ , its weight enumerator is given by

$$1 + 48z^6 + 30z^8 + 48z^{10} + z^{16}. \quad (7)$$

The set of 48 codewords of weight 6 of  $\mathcal{C}(f_1, f_2)$  is a union of the incidence matrices of three SDP designs from  $\mathcal{U}$  with

pairwise disjoint sets of blocks. A quick check shows that there are exactly 56 such collections of 48 codewords that generate a code having weight enumerator (7). Therefore, the number of distinct  $[16, 7, 6]$  subcodes of  $\text{RM}_2(1, 4)$  based on  $(4, 2)$  bent vectorial functions is 56. The  $7 \times 16$  generator matrix  $G$  of one such  $[16, 7, 6]$  code is listed below:

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

The first five rows of  $G$  form a generator matrix of  $\text{RM}_2(1, 4)$ , while the last two rows are codewords of weight 6 in  $\text{RM}_2(2, 4)$ . The full automorphism group of the  $[16, 7, 6]$  code generated by  $G$  is of order 5760. Since the order of the automorphism group of  $\text{RM}_2(1, 4)$  is 322560, and

$$322560/5760 = 56,$$

it follows that all 56  $[16, 7, 6]$  codes based on  $(4, 2)$  bent vectorial functions are pairwise equivalent.  $\square$

The next two examples illustrate that there are at least three inequivalent optimal  $[64, 10, 28]$  codes that are obtainable from bent vectorial functions from  $\text{GF}(2^6)$  to  $\text{GF}(2)^3$ . The parameters  $[64, 10, 28]$  correspond to  $m = 3$  in Note 6.

**Example 8.** The binary cyclic  $[63, 10]$  code  $\mathcal{C}$  with parity check polynomial  $h(x) = (x+1)(x^3+x^2+1)(x^6+x^5+x^4+x+1)$  has weight enumerator

$$1 + 196z^{27} + 252z^{28} + 63z^{31} + 63z^{32} + 252z^{35} + 196z^{36} + z^{63}.$$

The  $[63, 7]$  subcode  $\mathcal{C}'$  of  $\mathcal{C}$  having check polynomial  $h'(x) = (x+1)(x^6+x^5+x^4+x+1)$  has weight enumerator

$$1 + 63z^{31} + 63z^{32} + z^{63}.$$

The extended  $[64, 7]$  code  $(\mathcal{C}')^*$  of  $\mathcal{C}'$  has weight enumerator

$$1 + 126z^{32} + z^{64},$$

hence,  $(\mathcal{C}')^*$  is equivalent to the first order Reed-Muller code  $\text{RM}_2(1, 6)$ . The extended  $[64, 10]$  code  $\mathcal{C}^*$  of  $\mathcal{C}$  has weight enumerator given by

$$1 + 448z^{28} + 126z^{32} + 448z^{36} + z^{64}. \quad (8)$$

Since  $\mathcal{C}^*$  contains a copy of the first order Reed-Muller code  $\text{RM}_2(1, 6)$  as a subcode, it follows from Theorem 5 that  $\mathcal{C}^*$  can be obtained from a  $(6, 3)$  bent vectorial function from  $\text{GF}(2^6)$  to  $\text{GF}(2^3)$ . The full automorphism group of  $\mathcal{C}^*$  is of order

$$677,376 = 2^9 \cdot 3^3 \cdot 7^2.$$

Magma was used for these computations.

**Example 9.** Let  $M$  be the 7 by 64  $(0, 1)$ -matrix with the following structure: the  $i$ th column of the 6 by 64 submatrix  $M'$  of  $M$  consisting of its first six rows is the binary presentation of the number  $i$  ( $i = 0, 1, \dots, 63$ ), while the last row of  $M$  is the all-one row. Clearly,  $M$  is a generator matrix of a binary

linear [64, 7] code equivalent to the first order Reed-Muller code  $\text{RM}_2(1, 6)$ .

The first six rows of  $M$  can be viewed as the truth tables of the single Boolean variables  $x_1, x_2, \dots, x_6$ , while the seventh row of  $M$  is the truth table of the constant **1**.

We consider the Boolean bent functions given by

$$\begin{aligned} f_1(x_1, \dots, x_6) &= x_1x_6 + x_2x_5 + x_3x_4, \\ f_2(x_1, \dots, x_6) &= x_1x_5 + x_2x_4 + x_3x_5 + x_3x_6, \\ f_3(x_1, \dots, x_6) &= x_1x_4 + x_2x_5 + x_2x_6 + x_3x_4 + x_3x_5 + x_5x_6, \\ f_4(x_1, \dots, x_6) &= x_1x_4 + x_2x_3 + x_3x_6 + x_5x_6. \end{aligned}$$

The vectorial functions  $F_1 = (f_1, f_2, f_3)$ ,  $F_2 = (f_1, f_2, f_4)$  give via Theorem 5 binary linear codes  $\mathcal{C}_1, \mathcal{C}_2$  with parameters [64, 10, 28], having weight enumerator given by (8).

The automorphism groups of the codes  $\mathcal{C}_1, \mathcal{C}_2$  were computed using the computer-algebra package Magma [5].

The code  $\mathcal{C}_1$  has full automorphism group of order

$$10,752 = 2^9 \cdot 3 \cdot 7.$$

The code  $\mathcal{C}_2$  has full automorphism group of order

$$4,032 = 2^6 \cdot 3^2 \cdot 7.$$

Thus,  $\mathcal{C}_1, \mathcal{C}_2$  and the extended cyclic code  $\mathcal{C}^*$  from Example 8 are pairwise inequivalent.

We note that the code  $\mathcal{C}_1$  cannot be equivalent to any extended cyclic code because its group order is not divisible by 63.

**Note 10.** The full automorphism group of  $\mathcal{C}_1$  from Example 9 cannot be 2-transitive because its order is not divisible by 63. Thus, the code  $\mathcal{C}_1$  does not satisfy the classical sufficient condition to support 2-designs based on the 2-transitivity of its automorphism group (recall that according to [13], any 2-homogeneous group of degree 64 is necessarily 2-transitive).

In addition, the minimum distance of its dual code  $\mathcal{C}_1^\perp$  is 4, thus the Assmus-Mattson theorem guarantees only 1-designs to be supported by  $\mathcal{C}_1$ .

We will prove in the next section that all codes obtained from bent vectorial functions support 2-designs.

## V. A CONSTRUCTION OF 2-DESIGNS FROM BENT VECTORIAL FUNCTIONS

The following theorem establishes that the binary codes based on bent vectorial functions support 2-designs, despite that these codes do not meet the conditions of the Assmus-Mattson theorem for 2-designs.

**Theorem 11.** Let  $F(x) = (f_1(x), f_2(x), \dots, f_\ell(x))$  be a bent vectorial function from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^\ell$ , where  $m \geq 2$  and  $1 \leq \ell \leq m$ . Let  $\mathcal{C} = \mathcal{C}(f_1, \dots, f_\ell)$  be the binary linear code with parameters  $[2^{2m}, 2m + 1 + \ell, 2^{2m-1} - 2^{m-1}]$  defined in Theorem 5.

(a) The codewords of  $\mathcal{C}$  of minimum weight hold a 2-design  $\mathbb{D}$  with parameters

$$2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, (2^\ell - 1)(2^{2m-2} - 2^{m-1})). \quad (9)$$

(b) The codewords of  $\mathcal{C}$  of weight  $2^{2m-1} + 2^{m-1}$  hold a 2-design  $\overline{\mathbb{D}}$  with parameters

$$2 - (2^{2m}, 2^{2m-1} + 2^{m-1}, (2^\ell - 1)(2^{2m-2} + 2^{m-1})). \quad (10)$$

*Proof.* Since  $\mathcal{C}$  contains  $\text{RM}_2(1, 2m)$ , and the minimum distance of  $\text{RM}_2(1, 2m)^\perp$  is 4, the minimum distance  $d^\perp$  of  $\mathcal{C}^\perp$  is at least 4. Applying the MacWilliams transform (see, for example [23, p. 41]) to the weight enumerator (6) of  $\mathcal{C}$  shows that  $d^\perp = 4$ . It follows from the Assmus-Mattson theorem (Theorem 1) that the codewords of any given nonzero weight  $w < 2^{2m}$  in  $\mathcal{C}$  hold a 1-design.

However, we will prove that  $\mathcal{C}$  actually holds 2-designs, despite that the Assmus-Mattson theorem guarantees only 1-designs to be supported by  $\mathcal{C}$ .

Since the subcode  $\text{RM}_2(1, 2m)$  of  $\mathcal{C}$  contains all codewords of  $\mathcal{C}$  of weight  $2^{2m-1}$ , the codewords of this weight hold a 3-design  $\mathcal{A}$  with parameters  $3 - (2^{2m}, 2^{2m-1}, 2^{2m-2} - 1)$ . We note that  $\mathcal{A}$  is a 2-design with

$$\lambda_2 = \frac{2^{2m} - 2}{2^{2m-1} - 2} \cdot (2^{2m-2} - 1) = 2^{2m-1} - 1. \quad (11)$$

Let  $\mathbb{D}$  be the 1-design supported by codewords of weight  $2^{2m-1} - 2^{m-1}$ . Since the number of codewords of weight  $2^{2m-1} - 2^{m-1}$  is equal to  $(2^\ell - 1)2^{2m}$ ,  $\mathbb{D}$  is a 1-design with parameters  $1 - (2^{2m}, 2^{2m-1} - 2^{m-1}, (2^\ell - 1)(2^{2m-1} - 2^{m-1}))$ .

Every codeword of  $\mathcal{C}$  of weight  $2^{2m-1} + 2^{m-1}$  is the sum of a codeword of weight  $2^{2m-1} - 2^{m-1}$  and the all-one vector. Thus, the codewords of weight  $2^{2m-1} + 2^{m-1}$  hold a 1-design  $\overline{\mathbb{D}}$  having parameters  $1 - (2^{2m}, 2^{2m-1} + 2^{m-1}, (2^\ell - 1)(2^{2m-1} + 2^{m-1}))$ . Clearly,  $\overline{\mathbb{D}}$  is the complementary design of  $\mathbb{D}$ , that is, every block of  $\overline{\mathbb{D}}$  is the complement of some block of  $\mathbb{D}$ .

Let  $M$  be the  $2^{2m+1+\ell} \times 2^{2m}$  (0, 1)-matrix having as rows the codewords of  $\mathcal{C}$ . Since  $d^\perp = 4$ ,  $M$  is an orthogonal array of strength 3, that is, for every integer  $i$ ,  $1 \leq i \leq 3$ , and for every set of  $i$  distinct columns of  $M$ , every binary vector with  $i$  components appears exactly  $2^{2m+1+\ell-i}$  times among the rows of the  $2^{2m+1+\ell} \times i$  submatrix of  $M$  formed by the chosen  $i$  columns. In particular, any  $2^{2m+1+\ell} \times 2$  submatrix consisting of two distinct columns of  $M$  contains the binary vector  $(1, 1)$  exactly  $2^{2m+\ell-1}$  times as a row. Among these  $2^{2m+\ell-1}$  rows, one corresponds to the all-one codeword of  $\mathcal{C}$ ,  $2^{2m-1} - 1$  rows correspond to codewords of weight  $2^{2m-1}$  (by equation (11)), and the remaining

$$2^{2m+\ell-1} - 1 - (2^{2m-1} - 1) = (2^\ell - 1)2^{2m-1} \quad (12)$$

rows are labeled by codewords of weight  $2^{2m-1} \pm 2^{m-1}$ , corresponding to blocks of  $\mathbb{D}$  and  $\overline{\mathbb{D}}$ .

Let now  $1 \leq c_1 < c_2 \leq 2^{2m}$  be two distinct columns of  $M$ . These two columns label two distinct points of  $\mathbb{D}$  (resp.  $\overline{\mathbb{D}}$ ). Let  $\lambda$  denote the number of blocks of  $\mathbb{D}$  that are incident with  $c_1$  and  $c_2$ . Then the pair  $\{c_1, c_2\}$  is incident with

$$(2^\ell - 1)2^{2m} - 2(2^\ell - 1)(2^{2m-1} - 2^{m-1}) + \lambda = (2^\ell - 1)2^m + \lambda \quad (13)$$

blocks of the complementary design  $\overline{\mathbb{D}}$ . It follows from (13) and (12) that

$$(2^\ell - 1)2^m + 2\lambda = (2^\ell - 1)2^{2m-1},$$

whence

$$\lambda = (2^\ell - 1)(2^{2m-2} - 2^{m-1}),$$

and the statements (a) and (b) of the theorem follow.  $\square$

The special case  $\ell = 1$  in Theorem 11 implies as a corollary the following result of Dillon and Schatz [8].

**Theorem 12.** *Let  $f(x)$  be a bent function from  $GF(2^{2m})$  to  $GF(2)$ . Then the code  $\mathcal{C}(f)$  has parameters  $[2^{2m}, 2m + 2, 2^{2m-1} - 2^{m-1}]$  and weight enumerator (2). The minimum weight codewords form a symmetric SDP design with parameters (1).*

*Proof.* The weight enumerator (2) is obtained by substitution  $\ell = 1$  in (6). Since the number of minimum weight vectors is equal to the code length  $2^{2m}$ , the 2-design  $\mathbb{D}$  supported by the codewords of minimum weight is symmetric. Since every two blocks  $B_1, B_2$  of  $\mathbb{D}$  intersect in  $\lambda = 2^{2m-2} - 2^{m-1}$  points, the sum of the two codewords supporting  $B_1, B_2$  is a codeword  $c_{1,2}$  of weight  $2^{2m-1}$  that belongs to the subcode  $RM_2(1, 2m)$ .

Let  $B_3$  be a block distinct from  $B_1$  and  $B_2$ , and let  $c_3$  be the codeword associated with  $B_3$ . Since  $c_3$  is the truth table of a bent function, the sum  $c_{1,2} + c_3$  is a codeword of weight  $2^{2m-1} \pm 2^{m-1}$ , thus its support is either a block or the complement of a block of  $\mathbb{D}$ . Therefore,  $\mathbb{D}$  is an SDP design.  $\square$

**Theorem 13.** *The code  $\mathcal{C} = \mathcal{C}(f_1, \dots, f_\ell)$  from Theorem 11 is spanned by the set of codewords of minimum weight.*

*Proof.* All we need to prove is that the copy of  $RM_2(1, 2m)$  which is a subcode of  $\mathcal{C}$ , is spanned by some minimum weight codewords of  $\mathcal{C}$ .

It is known that the 2-rank (that is, the rank over  $GF(2)$ ) of the incidence matrix of any symmetric SDP design  $\mathbb{D}$  with  $2^{2m}$  points is equal to  $2m + 2$  (for a proof, see [12]). This implies that the binary code spanned by  $\mathbb{D}$  contains the first order Reed-Muller code  $RM_2(1, 2m)$ . Consequently the minimum weight vectors of the subcode  $\mathcal{C}_{f_1} = \mathcal{C}(f_1)$  of  $\mathcal{C} = \mathcal{C}(f_1, \dots, f_\ell)$  span the subcode of  $\mathcal{C}$  being equivalent to  $RM_2(1, 2m)$ .  $\square$

**Corollary 14.** *The two codes  $\mathcal{C}_f = \mathcal{C}(f_1, \dots, f_s)$  and  $\mathcal{C}_g = \mathcal{C}(g_1, \dots, g_s)$  obtained from bent vectorial functions  $F(f_1, \dots, f_s)$  and  $F(g_1, \dots, g_s)$  are equivalent if and only if the designs supported by their minimum weight vectors are isomorphic.*

**Example 15.** Let  $m = 5$ . Let  $w$  be a generator of  $GF(2^{10})^*$  with  $w^{10} + w^6 + w^5 + w^3 + w^2 + w + 1 = 0$ . Let  $\beta = w^{2^5+1}$ . Then  $\beta$  is a generator of  $GF(2^5)^*$ . Define  $\beta_j = \beta^j$  for  $1 \leq j \leq 5$ . Then  $\{\beta_1, \beta_2, \beta_3, \beta_4, \beta_5\}$  is a basis of  $GF(2^5)$  over  $GF(2)$ . Now consider the bent vectorial function  $(f_1, f_2, f_3, f_4, f_5)$  in Example 2 and the code  $\mathcal{C}(f_1, f_2, f_3)$ .

When  $i = 1$  and  $i = 7$ , the two codes  $\mathcal{C}(f_1, f_2, f_3)$  have parameters  $[1024, 14, 496]$  and weight enumerator

$$1 + 7168z^{496} + 2046z^{512} + 7168z^{528} + z^{1024}.$$

The two codes are not equivalent according to Magma. It follows from Corollary 14 that the two designs with

parameters  $2-(1024, 496, 1680)$  supported by these codes are not isomorphic.

**Note 16.** Examples 8 and 9 give three inequivalent [64, 10, 28] codes, and Example 15 lists two inequivalent codes with parameters  $[1024, 14, 496]$ , obtained from bent vectorial functions. As we pointed out in Note 10, the code  $\mathcal{C}_1$  from Example 9, does not have a 2-transitive group.

These examples, as well as further evidence provided by Theorem 18 below, suggest the following plausible statement that we formulate as a conjecture.

**Conjecture 17.** For any given  $\ell$  in the range  $1 \leq \ell \leq m$ , the number of inequivalent codes with parameters  $[2^{2m}, 2m + 1 + \ell, 2^{2m-1} - 2^{m-1}]$  obtained from  $(2m, \ell)$  bent vectorial functions via Theorem 5, grows exponentially with linear growth of  $m$ , and most of these codes do not admit a 2-transitive automorphism group.

As it is customary, by “most” we mean that the limit of the ratio of the number of 2-transitive codes divided by the total number of codes approaches zero when  $m$  grows to infinity.

The next theorem proves Conjecture 17 in the case  $\ell = 1$ .

**Theorem 18.** (i) *The number of inequivalent  $[2^{2m}, 2m + 2, 2^{2m-1} - 2^{m-1}]$  codes obtained from single bent functions from  $GF(2^{2m})$  to  $GF(2)$  grows exponentially with linear growth of  $m$ .*

(ii) *For every given  $m \geq 2$ , there is exactly one (up to equivalence) code with parameters  $[2^{2m}, 2m + 2, 2^{2m-1} - 2^{m-1}]$  obtained from a bent function from  $GF(2^{2m})$  to  $GF(2)$ , that admits a 2-transitive automorphism group.*

*Proof.* (i) By the Dillon-Schatz Theorem 12, the minimum weight codewords of a code  $\mathcal{C}(f)$  with parameters  $[2^{2m}, 2m + 2, 2^{2m-1} - 2^{m-1}]$  obtained from a bent function  $f$  form a symmetric SDP design  $\mathbb{D}(f)$  with parameters (1). It follows from Theorem 13 that two codes  $\mathcal{C}(f_1), \mathcal{C}(f_2)$  obtained from bent functions  $f_1, f_2$  are equivalent if and only if the corresponding designs  $\mathbb{D}(f_1), \mathbb{D}(f_2)$  are isomorphic. Since the number of nonisomorphic SDP designs with parameters (1) grows exponentially when  $m$  grows to infinity (Kantor [15]), the proof of part (i) is complete.

(ii) It follows from Theorem 13 that the automorphism group of a code  $\mathcal{C}(f)$  obtained from a bent function  $f$  coincides with the automorphism group of the design  $\mathbb{D}(f)$  supported by the codewords of minimum weight. The design  $\mathbb{D}(f)$  is a symmetric 2-design with parameters (1). It was proved by Kantor [17] that for every  $m \geq 2$ , there is exactly one (up to isomorphism) symmetric design with parameters (1) that admits a 2-transitive automorphism group. This completes the proof of part (ii).  $\square$

By Theorem 12, the codes based on single bent functions support symmetric 2-designs. The next theorem determines the block intersection numbers of the design  $\mathbb{D}(f_1, \dots, f_\ell)$  supported by the minimum weight vectors in the code  $\mathcal{C}(f_1, \dots, f_\ell)$  from Theorem 11.

**Theorem 19.** Let  $\mathbb{D} = \mathbb{D}(f_1, \dots, f_\ell)$ ,  $(1 \leq \ell \leq m)$ , be a 2-design with parameters

$$2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, (2^\ell - 1)(2^{2m-2} - 2^{m-1}))$$

supported by the minimum weight codewords of a code  $\mathcal{C} = \mathcal{C}(f_1, \dots, f_\ell)$  defined as in Theorem 11.

(a) If  $\ell = 1$ ,  $\mathbb{D}$  is a symmetric SDP design, with block intersection number  $\lambda = 2^{2m-2} - 2^{m-1}$ .

(b) If  $2 \leq \ell \leq m$ ,  $\mathbb{D}$  has the following three block intersection numbers:

$$\begin{aligned} s_1 &= 2^{2m-2} - 2^{m-2}, \quad s_2 = 2^{2m-2} - 2^{m-1}, \\ s_3 &= 2^{2m-2} - 3 \cdot 2^{m-2}. \end{aligned} \quad (14)$$

For every block of  $\mathbb{D}$ , these intersection numbers occur with multiplicities

$$\begin{aligned} n_1 &= 2^m(2^m + 1)(2^{\ell-1} - 1), \\ n_2 &= 2^{2m} - 1, \\ n_3 &= 2^m(2^m - 1)(2^{\ell-1} - 1). \end{aligned} \quad (15)$$

*Proof.* Case (a) follows from Theorem 12.

(b) Assume that  $2 \leq \ell \leq m$ . Let  $w_1, w_2$  be two distinct codewords of weight  $2^{2m-1} - 2^{m-1}$ . The Hamming distance  $d(w_1, w_2)$  between  $w_1$  and  $w_2$  is equal to

$$2(2^{2m-1} - 2^{m-1}) - 2s,$$

where  $s$  is the size of the intersection of the supports of  $w_1$  and  $w_2$ . Since the distance between  $w_1$  and  $w_2$  is either  $2^{2m-1} - 2^{m-1}$ , or  $2^{2m-1}$ , or  $2^{2m-1} + 2^{m-1}$ , the size  $s$  of the intersection of the two blocks of  $\mathbb{D}$  supported by  $w_1, w_2$  can take only the values  $s_i$ ,  $1 \leq i \leq 3$ , given by (14).

Let  $B$  be a block of  $\mathbb{D}$  supported by a codeword of weight  $2^{2m-1} - 2^{m-1}$ , and let  $n_i$ ,  $(1 \leq i \leq 3)$ , denote the number of blocks of  $\mathbb{D}$  that intersect  $B$  in  $s_i$  points. Let  $\mathbf{r} = (2^\ell - 1)$   $(2^{2m-1} - 2^{m-1})$  denote the number of blocks of  $\mathbb{D}$  containing a single point, and let  $b = (2^\ell - 1)2^{2m}$  denote the total number of blocks of  $\mathbb{D}$ . Finally, let  $k = 2^{2m-1} - 2^{m-1}$  denote the size of a block, and let  $\lambda = (2^\ell - 1)(2^{2m-2} - 2^{m-1})$  denote the number of blocks containing two points. We have

$$\begin{aligned} n_1 + n_2 + n_3 &= b - 1, \\ s_1 n_1 + s_2 n_2 + s_3 n_3 &= k(\mathbf{r} - 1), \\ s_1(s_1 - 1)n_1 + s_2(s_2 - 1)n_2 + s_3(s_3 - 1)n_3 &= k(k - 1)(\lambda - 1). \end{aligned}$$

The second and the third equation count in two ways the appearances of single points and ordered pairs of points of  $B$  in other blocks of  $\mathbb{D}$ . The unique solution of this system of equations for  $n_1, n_2, n_3$  is given by (15).  $\square$

**Note 20.** A bent set is a set  $S$  of bent functions such that the sum of every two functions from  $S$  is also a bent function [4]. Since every  $(2m, \ell)$  bent vectorial function gives rise to a bent set consisting of  $2^\ell$  functions [4, Proposition 1], it follows from [4, Theorem 1] that the set of blocks of the design  $\mathbb{D}$  is a union of  $2^\ell - 1$  linked system of symmetric  $2\text{-}(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$  designs. This gives an alternative proof of Theorem 11 and Theorem 19(b).

**Note 21.** For every  $m \geq 2$ , any code  $\mathcal{C}(f_1, f_2, \dots, f_m)$  based on a bent vectorial function  $F(x) = (f_1(x),$

$\dots, f_m(x))$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2^m)$ , contains  $2^m - 1$  subcodes  $\mathcal{C}' = \mathcal{C}'(f_{j_1}, \dots, f_{j_s})$ ,  $j_1 < \dots < j_s \leq m$ , such that

$$\text{RM}_2(1, 2m) \subset \mathcal{C}' \subseteq \mathcal{C}(f_1, \dots, f_m).$$

Each subcode  $\mathcal{C}'$  holds 2-designs. This may be the only known chain of linear codes, included in each other, other than the chain of the Reed-Muller codes,

$$\text{RM}_2(1, 2m) \subset \text{RM}_2(2, 2m) \subset \dots \subset \text{RM}_2(m - 2, 2m).$$

such that all codes in the chain support nontrivial 2-designs.

**Note 22.** We would demonstrate that the characterization of bent vectorial functions in Theorem 5 can be used to construct bent vectorial functions. To this end, consider the extended binary narrow-sense primitive BCH code of length  $2^{2m} - 1$  and designed distance  $2^{2m-1} - 1 - 2^{m-1}$ , which is affine-invariant and holds 2-designs [9]. This code has the desired weight enumerator of (6) for  $\ell = m$  [9]. It can be proved with the Delsarte theorem that the trace representation of this code is equivalent to the following code:

$$\left\{ (f_{a,b,h}(x))_{x \in \text{GF}(2^{2m})} : a \in \text{GF}(2^m), b \in \text{GF}(2^{2m}), h \in \text{GF}(2) \right\},$$

where

$$f_{a,b,h}(x) = \text{Tr}_{m/1} \left[ a \text{Tr}_{2m/m} \left( x^{1+2^{m-1}} \right) \right] + \text{Tr}_{2m/1}(bx) + h.$$

It then follows from Theorem 5 that  $\text{Tr}_{2m/m}(x^{1+2^{m-1}})$  is a bent vectorial function from  $\text{GF}(2^{2m})$  to  $\text{GF}(2^m)$ . Note that this bent vectorial function may not be new. But our purpose here is to show that bent vectorial functions could be constructed from special linear codes.

Conversely, we could say that the extended narrow-sense BCH code of length  $2^{2m} - 1$  and designed distance  $2^{2m-1} - 1 - 2^{m-1}$  is in fact generated from the bent vectorial function  $\text{Tr}_{2m/m}(x^{1+2^{m-1}})$  from  $\text{GF}(2^{2m})$  to  $\text{GF}(2^m)$  using the construction of Note 26.

Example 8 gives a demonstration of that. Thus, all known binary codes with the weight enumerator (6) for some  $1 \leq \ell \leq m$  and arbitrary  $m \geq 2$  are obtained from the bent vectorial function construction. As shown in Example 7, all  $[16, 7, 6]$  codes obtained from  $(4, 2)$  bent vectorial functions are equivalent. Example 9 shows that there are at least three inequivalent  $[64, 10, 28]$  binary codes from bent vectorial functions, one of these codes being an extended BCH code.

**Note 23.** It is known that two designs  $\mathbb{D}(f)$  and  $\mathbb{D}(g)$  from two single bent Boolean functions  $f$  and  $g$  on  $\text{GF}(2^{2m})$  are isomorphic if and only if  $f$  and  $g$  are weakly affinely equivalent [8]. Although the classification of bent Boolean functions into weakly affinely equivalent classes is open, the results from [15] and [8] imply that the number of nonisomorphic SDP designs and inequivalent bent functions in  $2m$  variables grows exponentially with linear growth of  $m$ .

**Note 24.** Two  $(n, \ell)$  vectorial Boolean functions  $(f_1(x), \dots, f_\ell(x))$  and  $(g_1(x), \dots, g_\ell(x))$  from  $\text{GF}(2^n)$  to  $\text{GF}(2)^\ell$  are said to be EA-equivalent if there are an automorphism of  $(\text{GF}(2^n), +)$ , a homomorphism  $L$  from  $(\text{GF}(2^n), +)$  to  $(\text{GF}(2)^\ell, +)$ , an  $\ell \times \ell$  invertible matrix  $M$  over

$\text{GF}(2)$ , an element  $a \in \text{GF}(2^n)$ , and an element  $b \in \text{GF}(2)^\ell$  such that

$$\begin{aligned} & (g_1(x), \dots, g_\ell(x)) \\ &= (f_1(A(x) + a), \dots, f_\ell(A(x) + a))M + L(x) + b \end{aligned}$$

for all  $x \in \text{GF}(2^n)$ .

Let  $(f_1(x), \dots, f_\ell(x))$  and  $(g_1(x), \dots, g_\ell(x))$  be two bent vectorial functions from  $\text{GF}(2^{2m})$  to  $\text{GF}(2)^\ell$ . We conjecture that the designs  $\mathbb{D}(f_1, \dots, f_\ell)$  and  $\mathbb{D}(g_1, \dots, g_\ell)$  are isomorphic if and only if  $(f_1(x), \dots, f_\ell(x))$  and  $(g_1(x), \dots, g_\ell(x))$  are EA-equivalent. The reader is invited to attack this open problem.

Suppose that  $\mathbb{D}$  is a 2-design with parameters (9) obtained from a bent vectorial function  $F(x) = (f_1(x), f_2(x), \dots, f_\ell(x))$ ,  $(1 \leq \ell \leq m)$ , via the construction from Theorem 11. Let  $\mathcal{B}$  be the block set of  $\mathbb{D}$ . If  $B$  is a block of  $\mathbb{D}$ , we consider the collection of new blocks  $\mathcal{B}^{de}$  consisting of intersections  $B \cap B'$  such that  $B' \in \mathcal{B}$  and  $|B \cap B'| = 2^{2m-2} - 2^{m-1}$ .

**Theorem 25.** *For each  $B \in \mathbb{D}$ , the incidence structure  $(B, \mathcal{B}^{de})$  is a quasi-symmetric design with parameters*

$$2 - (2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2} - 2^{m-1} - 1)$$

and intersection numbers  $2^{2m-3} - 2^{m-2}$  and  $2^{2m-3} - 2^{m-1}$ .

*Proof.* By Theorem 19, there are exactly  $2^{2m} - 1$  blocks that intersect  $B$  in  $2^{2m-2} - 2^{m-1}$  points. Together with  $B$ , these blocks form a symmetric SDP design  $D$  with parameters  $2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ . The incidence structure  $(B, \mathcal{B}^{de})$  is a derived design of  $D$ . It was proved in [12] that each derived design of a symmetric SDP  $2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$  design is quasi-symmetric design with intersection numbers  $2^{2m-3} - 2^{m-2}$  and  $2^{2m-3} - 2^{m-1}$ , and having the additional property that the symmetric difference of every two blocks is either a block or the complement of a block.  $\square$

**Note 26.** Let  $m > 1$  be an integer. Let  $F$  be a bent vectorial function from  $\text{GF}(2^{2m})$  to  $\text{GF}(2^m)$ . Let  $A$  be a subgroup of order  $2^s$  of  $(\text{GF}(2^m), +)$ . Define a binary code by

$$C_A := \left\{ (\text{Tr}_{m/1}(aF(x)) + \text{Tr}_{2m/1}(bx) + c)_{x \in \text{GF}(2^{2m})} : \begin{array}{l} a \in A, b \in \text{GF}(2^{2m}), c \in \text{GF}(2) \end{array} \right\}.$$

It can be shown that  $C_A$  can be viewed as a code  $C(f_{i_1}, \dots, f_{i_s})$  obtained from a bent vectorial function  $(f_{i_1}, \dots, f_{i_s})$ .

## VI. SUMMARY AND CONCLUDING REMARKS

The contributions of this paper are the following.

- A coding-theoretic characterization of bent vectorial functions (Theorem 5).
- A construction of a two-parameter family of four-weight binary linear codes with parameters  $[2^{2m}, 2m + 1 + \ell, 2^{2m-1} - 2^{m-1}]$  for all  $1 \leq \ell \leq m$  and all  $m \geq 2$ , obtained from  $(2m, \ell)$  bent vectorial functions (Theorem 11). The parameters of these codes appear to be new when  $2 \leq \ell \leq m - 1$ . This family of codes

includes some optimal codes, as well as codes meeting the BCH bound. These codes do not satisfy the conditions of the Assmus-Mattson theorem, but nevertheless hold 2-designs. It is plausible that most of these codes do not admit 2-transitive automorphism groups (Conjecture 17 and Theorem 18).

- A new construction of a two-parameter family of 2-designs with parameters

$$2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, (2^\ell - 1)(2^{2m-2} - 2^{m-1})), \quad (16)$$

and having three block intersection numbers, where  $2 \leq \ell \leq m$ , based on bent vectorial functions (Theorem 11 and Theorem 19). This construction is a generalization of the construction of SDP designs from single bent functions given in [8].

- The number of nonisomorphic designs with parameters (16) in the special case when  $\ell = 1$ , grows exponentially with  $m$  by a known theorem of Kantor [15]. It is an interesting open problem to prove that the number of nonisomorphic designs with parameters (16) grows exponentially for any fixed  $\ell > 1$ .

Finally, we would like to mention that vectorial Boolean functions were employed in a different way to construct binary linear codes in [20]. The codes from [20] have different parameters from the codes described in this paper.

## ACKNOWLEDGMENTS

Vladimir Tonchev would like to thank the Hong Kong University of Science and Technology for the kind hospitality and support during his visit, when a large portion of this paper was written. The authors wish to thank the anonymous reviewers for their valuable comments and suggestions for improving the manuscript.

## REFERENCES

- [1] E. F. Assmus, Jr., and J. D. Key, *Designs and Their Codes*. Cambridge, U.K.: Cambridge Univ. Press, 1992.
- [2] E. F. Assmus, Jr., and H. F. Mattson, Jr., “New 5-designs,” *J. Combinat. Theory*, vol. 6, no. 2, pp. 122–151, Mar. 1969.
- [3] T. Beth, D. Jungnickel, and H. Lenz, *Design Theory*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 1999.
- [4] C. Bey and G. M. Kyureghyan, “On Boolean functions with the sum of every two of them being bent,” *Des. Codes Cryptogr.*, vol. 49, nos. 1–3, pp. 341–346, Dec. 2008.
- [5] W. Bosma, J. Cannon, and C. Playoust, “The MAGMA algebra system I: The user language,” *J. Symbolic Comput.*, vol. 24, nos. 3–4, pp. 235–265, 1997.
- [6] C. Carlet and S. Mesnager, “Four decades of research on bent functions,” *Des. Codes Cryptogr.*, vol. 78, no. 1, pp. 5–50, Jan. 2016.
- [7] C. Carlet and S. Mesnager, “On the construction of bent vectorial functions,” *Int. J. Inf. Coding Theory*, vol. 1, no. 2, pp. 133–148, Mar. 2010.
- [8] J. F. Dillon and J. R. Schatz, “Block designs with the symmetric difference property,” in *Proc. NSA Math. Sci. Meetings*, R. L. Ward, Ed. 1987, pp. 159–164.
- [9] C. Ding and Z. Zhou, “Parameters of 2-designs from some BCH codes,” in *Codes, Cryptography Information Security* (Lecture Notes in Computer Science), vol. 10194, S. El Hajji, A. Nitaj, and E. M. Soudi, Eds. Cham, Switzerland: Springer, 2017, pp. 110–127.
- [10] M. Grassl. *Code Tables*. Accessed: Jun. 28, 2018. [Online]. Available: <http://www.codetables.de>
- [11] D. Jungnickel and V. D. Tonchev, “Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound,” *Des. Codes Cryptogr.*, vol. 1, no. 3, pp. 247–253, Sep. 1991.

- [12] D. Jungnickel and V. D. Tonchev, "On symmetric and quasi-symmetric designs with the symmetric difference property and their codes," *J. Combinat. Theory A*, vol. 59, no. 1, pp. 40–50, Jan. 1992.
- [13] W. M. Kantor, "Automorphism groups of designs," *Math. Zeitschrift*, vol. 109, no. 3, pp. 246–252, Jun. 1969.
- [14] W. M. Kantor, "Symplectic groups, symmetric designs, and line ovals," *J. Algebra*, vol. 33, no. 1, pp. 43–58, Jan. 1975.
- [15] W. M. Kantor, "Exponential numbers of two-weight codes, difference sets and symmetric designs," *Discrete Math.*, vol. 46, no. 1, pp. 95–98, Jan. 1983.
- [16] W. W. Kantor, "Homogeneous designs and geometric lattices," *J. Combinat. Theory A*, vol. 38, no. 1, pp. 66–74, Jan. 1985.
- [17] W. M. Kantor, "Classification of 2-transitive symmetric designs," *Graphs Combinatorics*, vol. 1, no. 1, pp. 165–166, Dec. 1985.
- [18] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North Holland, 1977.
- [19] S. Mesnager, *Bent Functions: Fundamentals and Results*. New York, NY, USA: Springer-Verlag, 2016.
- [20] D. Tang, C. Carlet, and Z. Zhou, "Binary linear codes from vectorial Boolean functions and their weight distribution," *Discrete Math.*, vol. 340, no. 12, pp. 3055–3072, 2017.
- [21] V. D. Tonchev, "Quasi-symmetric designs, codes, quadrics, and hyperplane sections," *Geometriae Dedicata*, vol. 48, no. 3, pp. 295–308, Dec. 1993.
- [22] V. D. Tonchev, "Combinatorial configurations," in *Longman Scientific and Technical*, Hoboken, NJ, USA: Wiley, 1988.
- [23] J. H. van Lint, *Introduction to Coding Theory*, 3rd ed. New York, NY, USA: Springer-Verlag, 1999.
- [24] G. Weng, R. Feng, and W. Qiu, "On the ranks of bent functions," *Finite Fields Their Appl.*, vol. 13, no. 4, pp. 1096–1116, Nov. 2007.
- [25] G. Weng, R. Feng, W. Qiu, and Z. Zheng, "The ranks of Maiorana–McFarland bent functions," *Sci. China A, Math.*, vol. 51, no. 9, pp. 1726–1731, Sep. 2008.

**Cunsheng Ding** (M'98–SM'05) was born in 1962 in Shaanxi, China. He received the M.Sc. degree in 1988 from the Northwestern Telecommunications Engineering Institute, Xian, China; and the Ph.D. in 1997 from the University of Turku, Turku, Finland.

From 1988 to 1992 he was a Lecturer of Mathematics at Xidian University, China. Before joining the Hong Kong University of Science and Technology in 2000, where he is currently a Professor of Computer Science and Engineering, he was an Assistant Professor of Computer Science at the National University of Singapore.

His research fields are combinatorial designs, cryptography and coding theory. He has coauthored five research monographs, and served as a guest editor or editor for ten journals. Dr. Ding co-received the State Natural Science Award of China in 1989.

**Akihiro Munemasa** was born in Chiba prefecture, Japan, on March 12, 1961. He received the B.Sci. and M.Sci. degrees from Sophia University, Tokyo, Japan, in 1983 and 1985, respectively, and the Ph.D. degree from Ohio State University, Columbus, in 1989. From 1989 to 1991 he was with the Department of Mathematics, Osaka Kyoiku University, Osaka, Japan as a Research Associate. He moved to Kyushu University, Fukuoka, Japan, in 1991 and was appointed there as an Associate Professor in 1994. Since 2003, he has been a Professor of Graduate School of Information Sciences, Tohoku University, Sendai, Japan. He had been one of the four Editors-in-Chief of *Journal of Algebraic Combinatorics* from 2000 to 2017, and then joined the team of Editors-in-Chief of the new journal *Algebraic Combinatorics* in 2018. His research interest includes algebraic coding theory, association schemes, combinatorial design theory, spectral graph theory, and permutation groups.

**Vladimir D. Tonchev** graduated with PhD in Mathematics from the University of Sofia, Bulgaria, in 1980, and received the Dr. of Mathematical Sciences degree from the Bulgarian Academy of Sciences in 1987. After spending a year as a research fellow at the Eindhoven University of Technology, The Netherlands, (1987–88), and two years at the universities of Munich, Heidelberg and Giessen in Germany as an Alexander von Humboldt Research Fellow (1988–90), Dr. Tonchev joined Michigan Technological University, where he is currently a Distinguished Professor. Tonchev has published over 180 papers, four books, three book chapters, and edited several volumes in the area of error-correcting codes, combinatorial designs, and their applications. Dr. Tonchev is a member of the editorial board of *Designs, Codes and Cryptography*, *Journal of Combinatorial Designs, Applications and Applied Mathematics*, and *Journal of Algebraic Combinatorics*.