Bent Vectorial Functions, Codes and Designs

Cunsheng Ding*, Akihiro Munemasa†, Vladimir Tonchev‡

August 28, 2018

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 [12], [7], [13], [10], [11]. The main objective of this paper is to use bent vectorial functions for the construction of a two-parameter family of binary linear codes that do not satisfy the conditions of the Assmus-Mattson theorem and do not admit 2-transitive or 2-homogeneous automorphism groups in general, but nevertheless hold 2-designs. A new coding-theoretic characterization of bent vectorial functions is presented.

Keywords: bent function, bent vectorial function, linear code, 2-design.
MSC: 94B05, 94B15, 05B05.

1 Introduction, motivations and objectives

We start with a brief review of combinatorial \(t\)-designs (cf. [1], [3], [18]). 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 \(\mathcal{D} = (\mathcal{P}, \mathcal{B})\) 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

---

*Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Hong Kong. Email: cding@ust.hk
†Research Center for Pure and Applied Mathematics, Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan. Email: munemasa@math.is.tohoku.ac.jp
‡Department of Mathematical Sciences, Michigan Technological University, Houghton, MI 49931, USA. Email: tonchev@mtu.edu
design is any isomorphism of the design to itself. The set of all automorphisms of a
design $\mathcal{D}$ form the (full) automorphism group of $\mathcal{D}$.

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 $\mathcal{D}$ 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 $\text{GF}(q)$, which is denoted by $C_q(\mathcal{D})$ 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 $C$ 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 $\mathcal{D} = \{\mathcal{P}, \mathcal{B}\}$ be a $2-(v, k, \lambda)$ symmetric design, where $\mathcal{B} = \{B_1, B_2, \cdots, B_v\}$
and $v \geq 2$. Then

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

If a symmetric design $\mathcal{D}$ has parameters
\begin{equation}
2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}),
\end{equation}
its derived designs have parameters
\begin{equation}
2 - (2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1}, 2^{2m-2} - 2^{m-1} - 1),
\end{equation}
and its residual designs have parameters
\begin{equation}
2 - (2^{2m-1} + 2^{m-1}, 2^{2m-2}, 2^{2m-2} - 2^{m-1}).
\end{equation}

A symmetric 2-design is said to have the symmetric difference property, or to be a
symmetric SDP design, (Kantor \cite{12, 13}), 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 a complement of a block. The
derived and residual designs of a symmetric SDP design are called quasi-symmetric
SDP designs \cite{11}. The binary codes of quasi-symmetric SDP give rise to an exponen-
tially growing number of inequivalent linear codes that meet the Grey-Rankin bound
\cite{10}. It was proved in \cite{17} 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 Dil- lon and Schatz [7], who proved that any symmetric SDP design with parameters \((1)\) is supported by the codewords of minimum weight in a binary linear code \(C\) of length \(2^m\), dimension \(2m + 2\) and weight enumerator given by

\[
1 + 2^{2m}z^{2m-1} - 2^{m-1} + (2^{2m+1} - 2)z^{2m-1} + 2^{2m}z^{2m-2} + 2^{m-1} + z^{2m},
\]

where \(C\) is spanned by the first order Reed-Muller code \(RM_2(1, 2m)\) and a vector \(u\) being the truth table of a bent function in \(2^m\) variables, or equivalently, \(u\) is the incidence vector of a Hadamard difference set in the additive group of \(GF(2)^{2m}\) with parameters

\[
(2^m, 2^{2m-1} \pm 2^{m-1}, 2^{2m-2} \pm 2^{m-1}).
\]

One of the objectives of this paper is to give a coding-theoretical characterization of bent vectorial functions (Theorem 5), that generalizes the Dillon and Schatz characterization of single bent functions [7]. Another objective is to present in Theorem 11 a two-parameter family of binary linear codes with parameters

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

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, and do not admit 2-transitive automorphism groups in general. The subclass of codes with \(\ell = 1\) consists of codes introduced by Dillon and Schatz [7] that are based on bent functions and support symmetric SDP designs. Examples of codes with \(\ell = m\) are given that are optimal or have the largest known minimum distance for the given length and dimension.

2 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. For example, the extended ternary Golay code and the extended binary Golay code support 5-designs because these codes are invariant under the 5-transitive Mathieu groups \(M_{12}\) and \(M_{24}\) respectively. Similarly, the codewords of any given weight in a binary Reed-Muller code support a 3-design because the Reed-Muller codes are invariant under the 3-transitive affine group.

Another sufficient condition is given by the Assmus-Mattson theorem. Let \(C\) be a \([v, \kappa, d]\) linear code over \(GF(q)\), and let \(A_i = A_i(C)\) be the number of codewords of Hamming weight \(i\) in \(C\) \((0 \leq i \leq v)\). For each \(k\) with \(A_k \neq 0\), let \(B_k\) denote the set of the supports of all codewords of Hamming weight \(k\) in \(C\), where the code coordinates are indexed by \(1, 2, \ldots, v\). Let \(P = \{1, 2, \ldots, v\}\). The following theorem, proved by Assumus and Mattson, provides sufficient conditions for the pair \((P, B_k)\) to be a \(t\)-design.
Theorem 1. (The Assmus-Mattson Theorem \cite{2}). Let $C$ be a binary $[v, \kappa, d]$ code, and let $d^\perp$ be the minimum weight of the dual code $C^\perp$. Suppose that $A_i = A_i(C)$ and $A_i^\perp = A_i(C^\perp)$, $0 \leq i \leq \kappa$, are the weight distributions of $C$ and $C^\perp$, respectively. Fix a positive integer $t$ with $t < d^\perp$, and let $s$ be the number of $i$ with $A_i^\perp \neq 0$ for $0 < i \leq \kappa - t$. If $s \leq d - t$, then

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

The parameter $\lambda$ of a $t$-$(v, w; \lambda)$ design supported by the codewords of weight $w$ in a binary code $C$ is determined by the equation (6).

\[ A_w = \lambda \binom{v}{t} / \binom{w}{t}, \quad (6) \]

3 Bent functions and bent vectorial functions

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

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

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

The Walsh transform of $f$ is defined by

\[ \hat{f}(w) = \sum_{x \in GF(2^n)} (-1)^{f(x) + \text{Tr}_{n/1}(wx)}, \quad (7) \]

where $w \in GF(2^n)$.

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

\[ g(x) = f(A(x) + a) + L(x) + b \]

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

A Boolean function $f$ from $GF(2^{2m})$ to $GF(2)$ is called a bent function if $|\hat{f}(w)| = 2^m$ for every $w \in GF(2^{2m})$. It is well known that a function $f$ from $GF(2^{2m})$ to $GF(2)$ is bent if and only if $S_f$ is a difference set in $(GF(2^{2m}), +)$ with parameters \cite{13}.

A Boolean function $f$ from $GF(2^{2m})$ to $GF(2)$ 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 $RM_2(1, 2m)$ \cite{14} Theorem 6, page 426). It follows that

\[ |S_f| = 2^{2m-1} \pm 2^{m-1}. \quad (8) \]
There are many constructions of bent functions. The reader is referred to [5] and [15] for detailed information about bent functions.

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

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

For another equivalent definition of bent vectorial functions, see [6] or [15, Chapter 12].

Bent vectorial functions exist only when $\ell \leq m$ (cf. [15, Chapter 12]). There are a number of known constructions of bent vectorial functions. The reader is referred to [5] and [15, Chapter 12] for detailed information. Below we present a specific construction of bent vectorial functions from [6].

**Example 2.** [6]. Let $m \geq 1$ be an odd integer, $\beta_1, \beta_2, \ldots, \beta_m$ be a basis of $\text{GF}(2^m)$ over $\text{GF}(2)$, and let $u \in \text{GF}(2^m) \setminus \text{GF}(2^2)$. Let $i$ be a positive integer with $\text{gcd}(2m, i) = 1$. Then

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

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 $F(x) = (f_1(x), \ldots, f_\ell(x))$ 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 $\text{Tr}_{\ell/1}(a F(x))$ 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. [15, Chapter 12]). Let $m > 1$ and $i \geq 1$ be integers such that $2m / \text{gcd}(i, 2m)$ is even. Then $\text{Tr}_{2m/m}(ax^{2^i+1})$ is bent if and only if $\text{gcd}(2^i+1, 2^m+1) \neq 1$ and $a \in \text{GF}(2^{2m})^* \setminus \langle \alpha^{\text{gcd}(2^i+1, 2^m+1)} \rangle$, where $\alpha$ is a generator of $\text{GF}(2^{2m})^*$.

**Example 4.** (cf. [15, Chapter 12]). Let $m > 1$ and $i \geq 1$ be integers such that $\text{gcd}(i, 2m) = 1$. 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 $\text{GF}(2^{2m})^*$.

4 A construction of codes from bent vectorial functions

Let $q = 2^m$, let $\text{GF}(q) = \{u_1, u_2, \ldots, u_q\}$, 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
The weight enumerator of RM_2(1,2m) is
\[ 1 + (2^{2m+1} - 2)z^{2^{m-1}} + z^{2^m}. \] (11)

Up to equivalence, RM_2(1,2m) is the unique linear binary code with parameters [2^{2m},2m+1,2^{2m-1}]. 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 RM_2(1,2m)_⊥ 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 \( F(x) = (f_1(x), f_2(x), \ldots, f_\ell(x)) \) be a \((2m,\ell)\) vectorial function from GF(2^m) to GF(2)^\ell. For each \( i, 1 \leq i \leq \ell \), we define a binary vector
\[ F_i = (f_i(u_1), f_i(u_2), \ldots, f_i(u_q)) \in GF(2)^{2^m}, \] (12)
which is the truth table of the Boolean function \( f_i(x) \).

Let \( \ell \) be an integer in the range \( 1 \leq \ell \leq m \). We now define a \((2m+1+\ell) \times 2^m\) matrix
\[ G = G(f_1,\ldots,f_\ell) = \begin{bmatrix} G_0 \\ F_1 \\ \vdots \\ F_\ell \end{bmatrix}, \] (13)
where \( G_0 \) is the generator matrix of RM_2(1,2m). Let \( C(f_1,\ldots,f_\ell) \) denote the binary code of length \( 2^m \) with generator matrix \( G(f_1,\ldots,f_\ell) \) given by (13). The dimension of the code has the following lower and upper bounds:
\[ 2m + 1 \leq \dim(C(f_1,\ldots,f_\ell)) \leq 2m + 1 + \ell. \]

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

**Theorem 5.** A \((2m,\ell)\) vectorial function \( F(x) = (f_1(x), f_2(x), \ldots, f_\ell(x)) \) from GF(2^m) to GF(2)^\ell is a bent vectorial function if and only if the code \( C(f_1,\ldots,f_\ell) \) with generator matrix \( G \) given by (13) has weight enumerator
\[ 1 + (2^\ell - 1)2^{2m}z^{2^{m-1}2^{m-1}} + 2(2^{2m} - 1)z^{2^{2m-1}2^{m-1}} + (2^\ell - 1)2^{2m}z^{2^{2m-1}2^{m-1}} + z^{2^m}. \] (14)
Proof. By the definition of $G$, the code $C(f_1, \ldots, f_\ell)$ contains the first-order Reed-Muller code $RM_2(1, 2m)$ as a subcode, having weight enumerator (14).

It follows from (13) that every codeword of $C(f_1, \ldots, f_\ell)$ must be the truth table of a Boolean function

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

(15)

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

Suppose that $F(x) = (f_1(x), f_2(x), \ldots, f_\ell(x))$ is a $(2m, \ell)$ bent vectorial function. When $(u_1, \ldots, u_\ell) = (0, \ldots, 0), (v_0, v_1, \ldots, v_{2m-1})$ 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 $RM_2(1, 2m)$. Whenever $(u_1, \ldots, u_\ell) \neq (0, \ldots, 0)$, it follows from (13) 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 $RM_2(1, 2m)$, the code $C(f_1, \ldots, f_\ell)$ is self-complementary, and the desired weight enumerator of $C(f_1, \ldots, f_\ell)$ follows.

Suppose that $C(f_1, \ldots, f_\ell)$ has weight enumerator given by (14). Then $C(f_1, \ldots, f_\ell)$ has dimension $2m + 1 + \ell$. Consequently, $\sum_{i=1}^\ell u_i f_i(x)$ is the zero function if and only if $(u_1, \ldots, u_\ell) = (0, \ldots, 0)$. 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 $u = (u_1, \ldots, u_\ell) \neq (0, \ldots, 0)$ and all $(v_0, v_1, \ldots, v_{2m-1}) \in \text{GF}(2)^{2m}$. 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 $(v_0, v_1, \ldots, v_{2m-1})$ runs over $\text{GF}(2)^{2m}$. Consequently, $F(x)$ is a bent vectorial function.

\[ \Box \]

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

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

In particular, if $m = 2$, any code $C(f_1, f_2)$ 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. [9]).

If $m = 3$, any code $C(f_1, f_2, f_3)$ based on a bent vectorial function from $\text{GF}(2^6)$ to $\text{GF}(2)^3$ has parameters $[64, 10, 28]$ and is optimal [9].

If $m = 4$, any code $C(f_1, \ldots, f_6)$ 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 [9].

The next example demonstrates that up to equivalence, there is exactly one [16, 7, 6] code that can be obtained from a $(4, 2)$ bent vectorial function $F(x) = (f_1(x), f_2(x))$ from $\text{GF}(2^4)$ to $\text{GF}(2)^2$. 


Example 7. The weight enumerator of the second order Reed-Muller code $R_{2M}^2(2,4)$ is given by

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

The truth table of a bent function $f$ from $GF(2^4)$ to $GF(2)$ is a codeword $c_f$ of $R_{2M}^2(2,4)$ of weight 6. The linear code $C(f)$ spanned by $c_f$ and $R_{2M}^2(1,4)$ is a sub-code of $R_{2M}^2(2,4)$ of dimension 6, having weight enumerator

$$1 + 16z^6 + 30z^8 + 16z^{10} + z^{16}. \quad (17)$$

The codewords of $C(f)$ of weight 6 form a symmetric $2-(16,6,2)$ SDP design, whose blocks correspond to the supports of 16 bent functions. If $f_1, f_2$ are two distinct bent functions, the intersection of the codes $C(f_1), C(f_2)$ consists of the first order Reed-Muller code $R_{2M}^2(1,4)$. It follows that the set of 448 codewords of weight 6 in $R_{2M}^2(2,4)$ 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 $C(f_1, f_2)$ is a $[16,7]$ code defined by a bent vectorial function $(f_1, f_2)$, its weight enumerator is given by

$$1 + 48z^6 + 30z^8 + 48z^{10} + z^{16}. \quad (18)$$

The set of 48 codewords of weight 6 of $C(f_1, f_2)$ 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 (18). Therefore, the number of distinct $[16,7,6]$ subcodes of $R_{2M}^2(1,4)$ 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:

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

The first five rows of $G$ form a generator matrix of $R_{2M}^2(1,4)$, while the last two rows are codewords of weight 6 in $R_{2M}^2(2,4)$. 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 $R_{2M}^2(1,4)$ 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.
Example 8. The binary cyclic $[63, 10]$ code $C$ with parity check polynomial $h(x) = (x + 1)(x^3 + x^2 + 1)(x^6 + x^5 + x^4 + x + 1)$ has weight enumerator

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

The $[63, 7]$ subcode $C'$ of $C$ 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 $(C')^*$ of $C'$ has weight enumerator

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

hence, $(C')^*$ is equivalent to the first order Reed-Muller code $RM_2(1, 6)$. The extended $[64, 10]$ code $C^*$ of $C$ has weight enumerator given by

$$1 + 448z^{28} + 126z^{32} + 448z^{36} + z^{64}. \quad (19)$$

Since $C^*$ contains a copy of the first order Reed-Muller code $RM_2(1, 6)$ as a subcode, it follows from Theorem 5 that $C^*$ can be obtained from a $(6, 3)$ bent vectorial function from $GF(2^6)$ to $GF(2^3)$. The full automorphism group of $C^*$ 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 $i$ ($i = 0, 1, \ldots, 63$), 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 $RM_2(1, 6)$.

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

We consider the Boolean bent functions given by

$$f_1(x_1, \ldots, x_6) = x_1x_6 + x_2x_5 + x_3x_4,$$
$$f_2(x_1, \ldots, x_6) = x_1x_5 + x_2x_4 + x_3x_5 + x_3x_6,$$
$$f_3(x_1, \ldots, x_6) = x_1x_4 + x_2x_5 + x_2x_6 + x_3x_4 + x_3x_5 + x_5x_6,$$
$$f_4(x_1, \ldots, x_6) = x_1x_4 + x_2x_3 + x_3x_6 + x_5x_6.$$ 

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 $C_1, C_2$ with parameters $[64, 10, 28]$, having weight enumerator given by (19).
The code $C_1$ has full automorphism group of order
$$10,752 = 2^9 \cdot 3 \cdot 7.$$ 

The code $C_2$ has full automorphism group of order
$$4,032 = 2^6 \cdot 3^2 \cdot 7.$$ 

Thus, $C_1$, $C_2$ and the the extended cyclic code $C^*$ from Example 8 are pairwise inequivalent.

We note that the code $C_2$ cannot be equivalent to any extended cyclic code because its group order is not divisible by 63.

**Note 10.** The full automorphism group of $C_2$ from Example 9 cannot be 2-transitive or 2-homogeneous because its order is not divisible by 63. Thus, the code $C_2$ does not satisfy the classical sufficient condition to support 2-designs based on the degree of transitivity of its automorphism group. In addition, the minimum distance of its dual code $C_2^\perp$ is 4, thus the Assmus-Mattson theorem guarantees only 1-designs to be supported by $C_2$.

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

## 5 A construction of 2-designs from bent vectorial functions

One of the main contributions of this paper is the following.

**Theorem 11.** Let $F(x) = (f_1(x), f_2(x), \ldots, f_\ell(x))$ 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 $C = C(f_1, \ldots, f_\ell)$ 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 $C$ of minimum weight hold a 2-design $D$ with parameters
$$2 - (2^{2m}, 2^{m-1} - 2^{m-1}, (2^\ell - 1)(2^{2m-2} - 2^{m-1})).$$

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

**Proof.** Since $C$ 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 $C^\perp$ is at least 4. Applying the MacWilliams transform (see, for example [19, p. 41]) to the weight enumerator (14) of $C$ 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 $C$ hold a 1-design. Since the subcode $\text{RM}_2(1, 2m)$ of $C$ contains all codewords of $C$ of weight $2^{2m-1}$, the codewords of this weight hold a 3-design $A$ with parameters $3 - (2^{2m}, 2^{2m-1}, 2^{2m-2} - 1)$. We note that $A$ is a 2-design with
$$\lambda_2 = \frac{2^{2m} - 2 - 2}{2^{2m-1} - 2} \cdot (2^{2m-2} - 1) = 2^{2m-1} - 1. \quad (22)$$
Let \( D \) 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 \((2^\ell - 1)2^m\), \( D \) is a 1-design with parameters \(1-(2^m, 2^{2m-1} - 2^{m-1}, (2^\ell - 1)(2^{2m-1} - 2^{m-1}))\).

Every codeword of \( C \) 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 \( D \) having parameters \(1-(2^m, 2^{2m-1} + 2^{m-1}, (2^\ell - 1)(2^{2m-1} + 2^{m-1}))\). Clearly, \( \overline{D} \) is the complementary design of \( D \), that is, every block of \( \overline{D} \) is the complement of some block of \( D \).

Let \( M \) be the \( 2^{2m+1+\ell} \times 2^m \) matrix having as rows the codewords of \( C \). 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 \( 2^{2m+1+\ell-1} \) times as a row. Among these \( 2^{2m+\ell-1} \) rows, one corresponds to the all-one codeword of \( C \), \( 2^{2m-1} - 1 \) rows correspond to codewords of weight \( 2^{2m-1} \) (by equation (22)), and the remaining
\[
2^{2m+\ell-1} - 1 - (2^{2m-1} - 1) = (2^\ell - 1)2^{2m-1} \tag{23}
\]
rows are labeled by codewords of weight \( 2^{2m-1} \pm 2^{m-1} \), corresponding to blocks of \( D \) and \( \overline{D} \).

Let now \( 1 \leq c_1 < c_2 \leq 2^m \) be two distinct columns of \( M \). These two columns label two distinct points of \( D \) (resp. \( \overline{D} \)). Let \( \lambda \) denote the number of blocks of \( D \) that are incident with \( c_1 \) and \( c_2 \). Then the pair \( \{c_1, c_2\} \) is incident with
\[
(2^\ell - 1)2^m - 2(2^\ell - 1)(2^{2m-1} - 2^{m-1}) + \lambda = (2^\ell - 1)2^m + \lambda \tag{24}
\]
blocks of the complementary design \( \overline{D} \). It follows from (24) and (25) that
\[
(2^\ell - 1)2^m + 2\lambda = (2^\ell - 1)2^{2m-1},
\]
whence
\[
\lambda = (2^\ell - 1)(2^{m-2} - 2^{m-1}),
\]
and the statements (a) and (b) of the theorem follow. \( \square \)

The special case \( \ell = 1 \) Theorem [11] implies as a corollary the following result of Dillon and Schatz [7].

**Theorem 12.** Let \( f(x) \) be a bent function from \( \text{GF}(2^m) \) to \( \text{GF}(2) \). Then the code \( C(f) \) has parameters \([2^m, 2m + 2, 2^{2m-1} - 2^{m-1}]\) and weight enumerator
\[
1 + 2^m z^{2^{2m-1} - 2^{m-1}} + 2(2^m - 1)z^{2^{2m-1}} + 2^m z^{2^{2m-1} + 2^{m-1}} + z^{2^m}. \tag{25}
\]
The minimum weight codewords form a symmetric SDP design with parameters [11].
Proof. The weight enumerator \( (14) \) is obtained by substitution \( \ell = 1 \) in \( (14) \). 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 \( \text{RM}_2(1,2m) \).

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 \( 2^{2m-1} + 2^{m-1} \), 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 \( C = C(f_1, \cdots, f_t) \) from Theorem 11 is spanned by the set of codewords of minimum weight.

Proof. All we need to prove is that the copy of \( \text{RM}_2(1,2m) \) which is a subcode of \( C \), is spanned by the minimum weight codewords of \( C \).

It is known that the 2-rank (that is, the rank over \( \text{GF}(2) \)) of the incidence matrix of any symmetric SDP design \( \mathbb{D} \) with \( 2^{2m} \) points is equal to \( 2m + 2 \) (for as proof, see [11]). This implies that the binary code spanned by \( \mathbb{D} \) contains the first order Reed-Muller code \( \text{RM}_2(1,2m) \). Consequently the minimum weight vectors of the subcode \( C_f = C(f_1) \) of \( C = C(f_1, \cdots, f_t) \) span the subcode of \( C \) being equivalent to \( \text{RM}(1,2m) \).

\[ \square \]

**Corollary 14.** Two codes \( C_f = C(f_1, \cdots, f_s) \), \( C_g = C(g_1, \cdots, g_s) \) obtained from bent vectorial functions \( F(f_1, \cdots, f_s), F(g_1, \cdots, g_s) \) 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 \( \text{GF}(2^{10})^* \) with \( w^{10} + w^6 + w^5 + w^3 + w^2 + w + 1 = 0 \). Let \( \beta = w^{25} + 1 \). Then \( \beta \) is a generator of \( \text{GF}(2^5)^* \). 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 \( \text{GF}(2^5) \) over \( \text{GF}(2) \). Now consider the bent vectorial function \( (f_1, f_2, f_3, f_4, f_5) \) in Example 2 and the code \( C(f_1, f_2, f_3) \).

When \( i = 1 \) and \( i = 7 \) in Example 2 the two codes \( C(f_1, f_2, f_3) \) 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.

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 \( \mathbb{D}(f_1, \cdots, f_t) \) supported by the minimum weight vectors in the code \( C(f_1, \cdots, f_t) \) from Theorem 11.
Theorem 16. Let $\mathbb{D} = \mathbb{D}(f_1, \ldots, f_\ell)$, $(1 \leq \ell \leq m)$, 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 $C = C(f_1, \ldots, f_\ell)$ 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:

$$s_1 = 2^{2m-2} - 2^{m-2}, s_2 = 2^{2m-2} - 2^{m-1}, s_3 = 2^{2m-2} - 3 \cdot 2^{m-2}.$$  \hfill (26)

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

$$n_1 = 2^{m}(2^m + 1)(2^{\ell-1} - 1), n_2 = 2^{2m} - 1, n_3 = 2^{m}(2^{m} - 1)(2^{\ell-1} - 1).$$  \hfill (27)

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 (26).

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 $r = (2^\ell - 1)(2^{2m-1} - 2^{m-1})$ denote the number of blocks of $\mathbb{D}$ containing a single point, and let $b = (2^\ell - 1)2^m$ 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

$$n_1 + n_2 + n_3 = b - 1,$$

$$s_1n_1 + s_2n_2 + s_3n_3 = k(r - 1),$$

$$s_1(s_1 - 1)n_1 + s_2(s_2 - 1)n_2 + s_3(s_3 - 1)n_3 = k(k - 1)(\lambda - 1).$$

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 (27). \qed

Note 17. 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 $2-(2^{2m}, 2^{2m-1} - 2^{m-1}, 2^{2m-2} - 2^{m-1})$ designs. This gives an alternative proof of Theorem [11] and Theorem [16](b).
For every integer $m \geq 2$, any code $C(f_1, f_2, \ldots, f_m)$ based on a bent vectorial function $F(x) = (f_1(x), f_2(x), \ldots, f_m(x))$ from $GF(2^m)$ to $GF(2^m)$, contains $2^m - 1$ subcodes $C' = C'(f_{j_1}, \ldots, f_{j_s})$, $j_1 < \cdots < j_s \leq m$, such that

\[ RM_{2}(1,2m) \subseteq C' \subseteq C(f_1, \ldots, f_m). \]

Each subcode $C'$ 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,

\[ RM_{2}(1,2m) \subseteq RM_{2}(2,2m) \subseteq \cdots \subseteq RM_{2}(m-2,2m), \]

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

We would like to mention that any code $C(f_1, f_2, \ldots, f_m)$ has the same weight enumerator as the extended binary narrow-sense primitive BCH code of length $2^m - 1$ and designed distance $2^m - 1 - 2^{m-1}$, which is affine-invariant and holds 2-designs \[3\]. However, for all $2 \leq s \leq m - 1$, the parameters of a code $C(f_{j_1}, \ldots, f_{j_s})$ and the associated design $D(f_{j_1}, \ldots, f_{j_s})$ having three block intersection numbers appear to be new.

The extended narrow-sense BCH code of length $2^m - 1$ and designed distance $2^m - 1 - 2^{m-1}$ is in fact generated from the bent vectorial function $\text{Tr}_{2m/m}(ax^{1+2^{m-1}})$ from $GF(2^m)$ to $GF(2^m)$ using the construction of Note \[21\]. Example \[8\] gives a demonstration of that. Thus, all known binary codes with the weight enumerator \[14\] 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.

It is known that two designs $D(f)$ and $D(g)$ from two single bent Boolean functions $f$ and $g$ on $GF(2^m)$ are isomorphic if and only if $f$ and $g$ are weakly affinely equivalent \[7\]. Although the classification of bent Boolean functions into weakly affinely equivalent classes is open, the results from \[13\] and \[7\] imply that the number of nonisomorphic SDP designs and inequivalent bent functions in $2m$ variables grows exponentially with linear growth of $m$.

Two $(n, \ell)$ vectorial Boolean functions $(f_1(x), \ldots, f_\ell(x))$ and $(g_1(x), \ldots, g_\ell(x))$ from $GF(2^n)$ to $GF(2^\ell)$ are said to be EA-equivalent if there are an automorphism of $(GF(2^n), +)$, a homomorphism $L$ from $(GF(2^n), +)$ to $(GF(2^\ell), +)$, an $\ell \times \ell$ invertible matrix $M$ over $GF(2)$, an element $a \in GF(2^n)$, and an element $b \in GF(2^\ell)$ such that

\[(g_1(x), \ldots, g_\ell(x)) = (f_1(A(x) + a), \ldots, f_\ell(A(x) + a))M + L(x) + b \quad (28)\]

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

Let $(f_1(x), \ldots, f_\ell(x))$ and $(g_1(x), \ldots, g_\ell(x))$ be two bent vectorial functions from $GF(2^{2m})$ to $GF(2^\ell)$. We conjecture that the designs $D(f_1, \ldots, f_\ell)$ and $D(g_1, \ldots, g_\ell)$ are isomorphic if and only if $(f_1(x), \ldots, f_\ell(x))$ and $(g_1(x), \ldots, g_\ell(x))$ are EA-equivalent. The reader is invited to attack this open problem.
Suppose that $D$ is a 2-design with parameters \([20]\) obtained from a bent vectorial function $F(x) = (f_1(x), f_2(x), \cdots, f_s(x))$, \((1 \leq \ell \leq m)\), via the construction from Theorem \([11]\). Let $B$ be the block set of $D$. If $B$ is a block of $D$, we consider the collection of new blocks $B^{de}$ consisting of intersections $B \cap B'$ such that $B' \in B$ and $|B \cap B'| = 2^{2m-2} - 2^{m-1}$.

**Theorem 22.** For each $B \in D$, the incidence structure $(B, B^{de})$ is a quasi-symmetric design with parameters

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

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

**Proof.** By Theorem \([16]\) 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 $(B, B^{de})$ is a derived design of $D$. It was proved in \([11]\) 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 a complement of a block. \(\square\)

**Note 23.** Let $m > 1$ be an integer. Let $F$ be a bent vectorial function from $\text{GF}(2^m)$ to $\text{GF}(2^m)$. Let $A$ be a subgroup of order $2^s$ of $\text{GF}(2^m, +)$. Define a binary code by

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

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

6 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 $\left[2^{2m}, 2m + 1 + s, 2^{2m-1} - 2^{m-1}\right]$ for all $1 \leq s \leq m$ and all $m \geq 2$, obtained from $(2m, m)$ bent vectorial functions (Theorem \([11]\)). The parameters of these codes appear to be new when $2 \leq s \leq m - 1$. 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, and do not admit 2-transitive or 2-homogeneous automorphism groups in general, but nevertheless hold 2-designs.
• A new construction of a two-parameter family of 2-designs with parameters
\[ 2 - (2^{2m}, 2^{2m-1} - 2^{m-1}, (2^s - 1)(2^{2m-2} - 2^{m-1})) \]
and having three block intersection numbers, where \( 2 \leq s \leq m \) and \( m \geq 2 \), based on bent vectorial functions (Theorem [11]). This construction is a generalization of the construction of SDP designs from single bent functions given in [7].

Finally, we would like to mention that vectorial Boolean functions were employed in a different way to construct binary linear codes in [16]. The codes from [16] have different parameters from the codes described in this paper.

References

[1] Assmus, Jr. E. F., Key, J. D.: Designs and Their Codes. Cambridge University Press, Cambridge (1992).

[2] Assmus, Jr. E.F , Mattson, Jr. H.F .: New 5-designs, J. Comb. Theory 6, 122–151 (1969).

[3] Beth T., Jungnickel, D., Lenz, H.: Design Theory, 2nd Ed., Cambridge University Press, Cambridge 1999.

[4] Bey, C., Kyureghyan, G. M.: On Boolean functions with the sum of every two of them being bent. Des. Codes Cryptogr. 49 341–346 (2008).

[5] Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. 78 5–50 (2016).

[6] Carlet, C., Mesnager, S.: On the construction of bent vectorial functions. International Journal of Information and Coding Theory 1 133–148 (2010).

[7] Dillion, J. F., Schatz, J. R.: “Block designs with the symmetric difference property,” in: Proc. of the NSA Mathematical Sciences Meetings, (Ward R. L. Ed.), pp. 159–164.

[8] Ding, C., Zhou, Z.: “Parameters of 2-designs from some BCH codes,” in: S. El Hajji, A. Nitaj and E. M. Souidi (Eds.), Codes, Cryptography and Information Security, Lecture Notes in Computer Science, Vol. 10194, pp. 110–127, Springer, 2017.

[9] Grassl, M.: Code Tables, www.codetables.de.

[10] Jungnickel, D., Tonchev, V. D.: Exponential number of quasi-symmetric SDP designs and codes meeting the Grey-Rankin bound. Designs, Codes and Cryptography 1, 247–253 (1991).
[11] Jungnickel, D., Tonchev, V. D.: On symmetric and quasi-symmetric designs with the symmetric difference property and their codes. J. Comb. Theory A 59, 40–50 (1992).

[12] Kantor, W. M.: Symplectic groups, symmetric designs, and line ovals. J. Algebra 33, 43–58 (1975).

[13] Kantor, W. M.: Exponential number of two-weight codes, difference sets and symmetric designs. Disc. Math. 46, 95–98 (1983).

[14] MacWilliams F.J., Sloane, N.J.A.: The Theory of Error-Correcting Codes, North Holland, 1977.

[15] Mesnager, S.: Bent Functions: Fundamentals and Results. Springer Verlag, Switzerland (2016).

[16] Tang, D., Carlet, C., Zheng, Z.: Binary linear codes from vectorial boolean functions and their weight distribution. Discrete Mathematics 340, 3053–3072 (2017).

[17] Tonchev, V. D.: Quasi-symmetric designs, codes, quadrics, and hyperplane sections. Geometriae Dedicata 48, 295–308 (1993).

[18] Tonchev, V.D.: Combinatorial configurations, Longman Scientific and Technical, Wiley, New York 1988.

[19] Van Lint, J. H.: Introduction to Coding Theory, Third Edition. Springer Verlag, New York (1999).

[20] Weng, G., Feng, R., Qiu, W.: On the ranks of bent functions. Finite Fields Appl. 13, 1096–1116 (2007).

[21] Weng, G., Feng, R., Qiu, W., Zheng Z.: The ranks of Maiorana-McFarland bent functions. Sci. China Ser. A 51, 1726–1731 (2008).