Noname manuscript No.
(will be inserted by the editor)

Combinatorial t-designs from special functions

Cunsheng Ding · **Chunming Tang**

Received: date / Accepted: date

Abstract A special function is a function either of special form or with a special property. Special functions have interesting applications in coding theory and combinatorial t-designs. The main objective of this paper is to survey t-designs constructed from special functions, including quadratic functions, almost perfect nonlinear functions, almost bent functions, bent functions, bent vectorial functions, and planar functions. These combinatorial designs are not constructed directly from such functions, but come from linear codes which are constructed with such functions. As a byproduct, this paper also surveys linear codes from certain special functions.

Keywords Cyclic code · design · linear code · special function

1 Introduction

Let $\mathcal{P}$ be a set of $v \geq 1$ elements, and let $\mathcal{B}$ be a set of k-subsets of $\mathcal{P}$, where k is a positive integer with $1 \leq k \leq v$. Let t be a positive integer with $t \leq k$. The pair $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ is called a t-(v,k,λ) *design*, or simply t*-design*, if every t-subset of $\mathcal{P}$ is contained in exactly λ elements of $\mathcal{B}$. The elements of $\mathcal{P}$ are called points, and those of $\mathcal{B}$ are referred to as blocks. 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 repeated blocks. In this survey, we consider only simple t-designs. A t-design is called *symmetric* if $v = b$. It is clear that t-designs with $k = t$ or $k = v$ always exist. Such t-designs are *trivial*. In this survey, we consider only t-designs with $v > k > t$. A t-(v,k,λ) design is referred to as a *Steiner system* if $t \geq 2$ and $\lambda = 1$, and is denoted by $S(t,k,v)$.

C. Ding's research was supported by the Hong Kong Research Grants Council, Proj. No. 16300418. C. Tang was supported by National Natural Science Foundation of China (Grant No. 11871058) and China West Normal University (14E013, CXTD2014-4 and the Meritocracy Research Funds).

Cunsheng Ding
Department of Computer Science and Engineering, The Hong Kong University of Science and Technology,
Clear Water Bay, Kowloon, Hong Kong, China
Tel.: +852-2358 7021, Fax: +852-2358 1477, E-mail: cding@ust.hk

Chunming Tang
The School of Mathematics and Information, China West Normal University, Nanchong 637002, China
E-mail: tangchunmingmath@163.com

We assume that the reader is familiar with the basics of linear codes and cyclic codes, and proceed to introduce the classical construction of t-designs from codes directly. Let C be a $[v, \kappa, d]$ linear code over $\mathrm{GF}(q)$. Let $A_i := A_i(\mathsf{C})$, which denotes the number of codewords with Hamming weight i in C, where $0 \le i \le v$. The sequence $(A_0, A_1, \cdots, A_v)$ is called the *weight distribution* of C, and $\sum_{i=0}^{v} A_i z^i$ is referred to as the *weight enumerator* of C. For each k with $A_k \neq 0$, let $\mathcal{B}_k$ denote the set of the supports of all codewords with Hamming weight k in C, where the coordinates of a codeword are indexed by $(0, 1, 2, \cdots, v-1)$. Let $\mathcal{P} = \{0, 1, 2, \cdots, v-1\}$. The pair $(\mathcal{P}, \mathcal{B}_k)$ may be a t-(v, k, λ) design for some positive integer λ, which is called a *support design* of the code. In such a case, we say that the code C holds a t-(v, k, λ) design. Throughout this paper, we denote the dual code of C by $\mathsf{C}^\perp$, and the extended code of C by $\overline{\mathsf{C}}$.

The following theorem, developed by Assumus and Mattson, shows that the pair $(\mathcal{P}, \mathcal{B}_k)$ defined by a linear code is a t-design under certain conditions [1], [22, p. 303].

Theorem 1 (Assmus-Mattson Theorem) *Let C be a $[v, k, d]$ code over $\mathrm{GF}(q)$. Let $d^\perp$ denote the minimum distance of $\mathsf{C}^\perp$. Let w be the largest integer satisfying $w \le v$ and*

$$w - \left\lfloor \frac{w+q-2}{q-1} \right\rfloor < d.$$

Define $w^\perp$ analogously using $d^\perp$. Let $(A_i)_{i=0}^{v}$ and $(A_i^\perp)_{i=0}^{v}$ denote the weight distribution of C and $\mathsf{C}^\perp$, respectively. Fix a positive integer t with $t < d$, and let s be the number of i with $A_i^\perp \neq 0$ for $0 \le i \le v-t$. Suppose $s \le d-t$. Then

- *the codewords of weight i in C hold a t-design provided $A_i \neq 0$ and $d \le i \le w$, and*
- *the codewords of weight i in $\mathsf{C}^\perp$ hold a t-design provided $A_i^\perp \neq 0$ and $d^\perp \le i \le \min\{v-t, w^\perp\}$.*

The Assmus-Mattson Theorem is a very useful tool in constructing t-designs from linear codes, and has been recently employed to construct infinitely many 2-designs and 3-designs in [15], [13] and [14].

The automorphism group of a linear code may show that a linear code holds t-designs. To introduce this approach, we have to define the automorphism group of linear codes.

The set of coordinate permutations that map a code C to itself forms a group, which is referred to as the *permutation automorphism group* of C and denoted by $\mathrm{PAut}(\mathsf{C})$. If C is a code of length n, then $\mathrm{PAut}(\mathsf{C})$ is a subgroup of the *symmetric group* Sym_n.

A *monomial matrix* over $\mathrm{GF}(q)$ is a square matrix having exactly one nonzero element of $\mathrm{GF}(q)$ in each row and column. A monomial matrix M can be written either in the form DP or the form PD_1, where D and D_1 are diagonal matrices and P is a permutation matrix.

The set of monomial matrices that map C to itself forms the group $\mathrm{MAut}(\mathsf{C})$, which is called the *monomial automorphism group* of C. Clearly, we have

$$\mathrm{PAut}(\mathsf{C}) \subseteq \mathrm{MAut}(\mathsf{C}).$$

The *automorphism group* of C, denoted by $\mathrm{Aut}(\mathsf{C})$, is the set of maps of the form $M\gamma$, where M is a monomial matrix and γ is a field automorphism, that map C to itself. In the binary case, $\mathrm{PAut}(\mathsf{C})$, $\mathrm{MAut}(\mathsf{C})$ and $\mathrm{Aut}(\mathsf{C})$ are the same. If q is a prime, $\mathrm{MAut}(\mathsf{C})$ and $\mathrm{Aut}(\mathsf{C})$ are identical. In general, we have

$$\mathrm{PAut}(\mathsf{C}) \subseteq \mathrm{MAut}(\mathsf{C}) \subseteq \mathrm{Aut}(\mathsf{C}).$$

By definition, every element in $\mathrm{Aut}(\mathsf{C})$ is of the form $DP\gamma$, where D is a diagonal matrix, P is a permutation matrix, and γ is an automorphism of $\mathrm{GF}(q)$. The automorphism group $\mathrm{Aut}(\mathsf{C})$ is said to be t-transitive if for every pair of t-element ordered sets of coordinates, there is an element $DP\gamma$ of the automorphism group $\mathrm{Aut}(\mathsf{C})$ such that its permutation part P sends the first set to the second set.

A proof of the following theorem can be found in [22, p. 308].

Theorem 2 *Let C be a linear code of length n over $\mathrm{GF}(q)$ where $\mathrm{Aut}(\mathsf{C})$ is t-transitive. Then the codewords of any weight $i \geq t$ of C hold a t-design.*

This theorem gives another sufficient condition for a linear code to hold t-designs. To apply Theorem 2, we have to determine the automorphism group of C and show that it is t-transitive. It is in general very hard to find out the automorphism group of a linear code. Even if we know that a linear code holds t-(v,k,λ) designs, determining the parameters k and λ could be extremely difficult.

Most t-designs held in linear codes have been proved either by the Assmus-Mattson Theorem or the automorphism groups of the codes. However, the support designs of some linear codes are proved with other approaches, and cannot be proved with any of the two approaches above. We will see such designs in the sequel.

Special functions can be employed in different ways to construct codes, which hold t-designs. The main objective of this paper is to survey support designs of linear codes from special functions such as quadratic functions, almost bent functions, almost perfect nonlinear function, bent functions, bent vectorial functions, and planar functions. As a byproduct, this paper also summarises linear codes which are constructed with such functions. Some new results are also presented in this paper.

Let $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ be a t-(v,k,λ) design with $b \geq 1$ blocks. The points of $\mathcal{P}$ are usually indexed with $p_1, p_2, \cdots, p_v$, and the blocks of $\mathcal{B}$ are normally denoted by $B_1, B_2, \cdots, B_b$. The *incidence matrix* $M_{\mathbb{D}} = (m_{ij})$ of $\mathbb{D}$ is a $b \times v$ matrix where $m_{ij} = 1$ if p_j is on B_i and $m_{ij} = 0$ otherwise. The binary matrix $M_{\mathbb{D}}$ is viewed as a matrix over $\mathrm{GF}(q)$ for any prime power q, and its row vectors span a linear code of length v over $\mathrm{GF}(q)$, which is denoted by $\mathsf{C}_q(\mathbb{D})$ and called the *classical code* of $\mathbb{D}$ over $\mathrm{GF}(q)$. It is clear that the code $\mathsf{C}_q(\mathbb{D})$ depends on the labelling of the points and blocks of $\mathbb{D}$, but is unique up to row and column permutations.

In this survey, we start with a special function f, then construct a linear code C_f over $\mathrm{GF}(q)$, and consider a support design $\mathbb{D}$ of C_f, and finally consider the linear code of the support design $\mathbb{D}$ over $\mathrm{GF}(r)$, i.e.,

$$f \longrightarrow \mathsf{C}_f \longrightarrow \mathbb{D} \longrightarrow \mathsf{C}_r(\mathbb{D}).$$

When $r = q$, the two codes C_f and $\mathsf{C}_r(\mathbb{D})$ are closely related. In particular, when $r = q = 2$, the code $\mathsf{C}_r(\mathbb{D})$ is a subcode of the original code C_f. When $r = q > 2$, the two codes may be related in a complex way. In this survey, we will also provide information on the code $\mathsf{C}_q(\mathbb{D})$ if this is possible.

2 Auxiliary results

The next theorem will be employed later and is a very useful and general result [28, p. 165].

Theorem 3 *Let C be an $[n,k,d]$ binary linear code with $k > 1$, such that for each weight $w > 0$ the supports of the codewords of weight w form a t-design, where $t < d$. Then the supports of the codewords of each nonzero weight in $\mathsf{C}^{\perp}$ also form a t-design.*

To determine the parameters of some t-designs, we will need the following lemma, which is a variant of the MacWilliams Identity [33, p. 41].

Theorem 4 *Let* C *be a* $[v,\kappa,d]$ *code over* $\mathrm{GF}(q)$ *with weight enumerator* $A(z)=\sum_{i=0}^{v}A_iz^i$ *and let* $A^{\perp}(z)$ *be the weight enumerator of* $\mathsf{C}^{\perp}$*. Then*

$$A^{\perp}(z)=q^{-\kappa}\Big(1+(q-1)z\Big)^{v}A\Big(\frac{1-z}{1+(q-1)z}\Big).$$

We will need the following lemma whose proof is easy.

Theorem 5 *Let* C *be an* $[n,\kappa,d]$ *code over* $\mathrm{GF}(q)$ *with generator matrix G. Let H denote a generator matrix of its dual* $\mathsf{C}^{\perp}$ *with parameters* $[n,n-\kappa,d^{\perp}]$*. Then we have the following:*

- *The code* $\overline{\mathsf{C}^{\perp}}^{\perp}$ *has parameters* $[n+1,\kappa+1]$ *and generator matrix*

$$\begin{bmatrix}\mathbf{1} & 1\\ G & \mathbf{0}\end{bmatrix},$$

where $\mathbf{1}=(111\cdots1)$ *is the all-one vector of length n,* $\mathbf{0}=(000\cdots0)^T$*, which is a column vector of length* κ*.*

- *The code* $\overline{\mathsf{C}}^{\perp}$ *has parameters* $[n+1,n+1-\kappa]$ *and generator matrix*

$$\begin{bmatrix}\mathbf{1} & 1\\ H & \mathbf{0}\end{bmatrix},$$

where $\mathbf{1}=(111\cdots1)$ *is the all-one vector of length n,* $\mathbf{0}=(000\cdots0)^T$*, which is a column vector of length* $n-\kappa$*.*

Let $f=f(x)$ be a Boolean function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$. The *support* D_f of f is defined as

$$D_f=\{x\in\mathrm{GF}(2^m):f(x)=1\}\subseteq\mathrm{GF}(2^m).$$

The $(0,1)$ incidence vector of D_f, having its coordinates labelled by the elements of $\mathrm{GF}(2^m)$, is called the *truth table* of f.

The *Walsh transform* of f is defined by

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

where $w\in\mathrm{GF}(2^m)$.

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

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

for all $x\in\mathrm{GF}(2^m)$.

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

$$(2^m,2^{m-1}\pm2^{(m-2)/2},2^{m-2}\pm2^{(m-2)/2}). \tag{2}$$

It follows that

$$|D_f|=2^{m-1}\pm2^{(m-2)/2}. \tag{3}$$

There are many constructions of bent functions. The reader is referred to [6] and [30] for detailed information about bent functions.

3 Affine-invariant codes from quadratic functions and their designs

In this section, we introduce a family of affine-invariant linear codes which are also extended cyclic codes. We order the elements of $\mathrm{GF}(q^m)$ and $\mathrm{GF}(q^m)^*$ as

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{q^m-2}, 0\}$$

and

$$\{1, \alpha, \alpha^2, \ldots, \alpha^{q^m-2}\},$$

respectively, where α is a primitive element of $\mathrm{GF}(q^m)$. Throughout this section, let $\mathrm{Tr}(x)$ be the trace function from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q)$.

Let t be a positive integer, and let f_i be a polynomial over $\mathrm{GF}(q^m)$ with $f_i(0) = 0$ and $1 \leq \deg(f_i) \leq q^m - 2$ for $1 \leq i \leq t$. For $\mathbf{f} = (f_1, \cdots, f_t)$, we define two related linear codes over $\mathrm{GF}(q)$ by

$$\mathsf{C}_{\mathbf{f}} = \left\{ \left(\mathrm{Tr}\left(\sum_{i=1}^{t} a_i f_i(x) \right) + h \right)_{x \in \mathrm{GF}(q^m)} : a_i \in \mathrm{GF}(q^m),\ h \in \mathrm{GF}(q) \right\} \tag{4}$$

and

$$\mathsf{C}_{\mathbf{f}}^* = \left\{ \left(\mathrm{Tr}\left(\sum_{i=1}^{t} a_i f_i(x) \right) \right)_{x \in \mathrm{GF}(q^m)^*} : a_i \in \mathrm{GF}(q^m) \right\}. \tag{5}$$

By definition, $\mathsf{C}_{\mathbf{f}}$ and $\mathsf{C}_{\mathbf{f}}^*$ are a linear code over $\mathrm{GF}(q)$ with length q^m and $q^m - 1$, respectively. Their dimensions satisfy $\dim(\mathsf{C}_{\mathbf{f}}) \leq tm + 1$ and $\dim(\mathsf{C}_{\mathbf{f}}^*) \leq tm$. The two codes $\mathsf{C}_{\mathbf{f}}$ and $\mathsf{C}_{\mathbf{f}}^*$ are related in the following way.

Theorem 6 *Let notation be the same as before. Then* $\mathsf{C}_{\mathbf{f}} = \overline{(\mathsf{C}_{\mathbf{f}}^*)^{\perp}}^{\perp}$. *Further,* $\dim(\mathsf{C}_{\mathbf{f}}) = \dim(\overline{\mathsf{C}_{\mathbf{f}}^*}) + 1$, *and* $\overline{\mathsf{C}_{\mathbf{f}}^*}$ *is a subcode of* $\mathsf{C}_{\mathbf{f}}$.

Proof Define

$$G = \begin{bmatrix} \mathrm{Tr}(\alpha^0 f_1(\alpha^0)) & \mathrm{Tr}(\alpha^0 f_1(\alpha^1)) & \cdots & \mathrm{Tr}(\alpha^0 f_1(\alpha^{q^m-2})) \\ \mathrm{Tr}(\alpha^1 f_1(\alpha^0)) & \mathrm{Tr}(\alpha^1 f_1(\alpha^1)) & \cdots & \mathrm{Tr}(\alpha^1 f_1(\alpha^{q^m-2})) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}(\alpha^{m-1} f_1(\alpha^0)) & \mathrm{Tr}(\alpha^{m-1} f_1(\alpha^1)) & \cdots & \mathrm{Tr}(\alpha^{m-1} f_1(\alpha^{q^m-2})) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}(\alpha^0 f_t(\alpha^0)) & \mathrm{Tr}(\alpha^0 f_t(\alpha^1)) & \cdots & \mathrm{Tr}(\alpha^0 f_t(\alpha^{q^m-2})) \\ \mathrm{Tr}(\alpha^1 f_t(\alpha^0)) & \mathrm{Tr}(\alpha^1 f_t(\alpha^1)) & \cdots & \mathrm{Tr}(\alpha^1 f_t(\alpha^{q^m-2})) \\ \vdots & \vdots & \vdots & \vdots \\ \mathrm{Tr}(\alpha^{m-1} f_t(\alpha^0)) & \mathrm{Tr}(\alpha^{m-1} f_t(\alpha^1)) & \cdots & \mathrm{Tr}(\alpha^{m-1} f_t(\alpha^{q^m-2})) \end{bmatrix}.$$

Then G is a generator matrix of $\mathsf{C}_{\mathbf{f}}^*$, though the rank of G could be less than tm.

Notice that $f_i(0) = 0$ for $1 \leq i \leq t$. By the ordering of the elements in $\mathrm{GF}(q^m)$ and $\mathrm{GF}(q^m)^*$ and the definition of the two codes $\mathsf{C}_{\mathbf{f}}^*$ and $\mathsf{C}_{\mathbf{f}}$ in (4) and (5), $\mathsf{C}_{\mathbf{f}}$ has the following generator matrix

$$\begin{bmatrix} \mathbf{1} & 1 \\ G & \mathbf{0} \end{bmatrix},$$

where $\mathbf{1} = (111\cdots 1)$ is the all-one vector of length q^m-1, $\mathbf{0} = (000\cdots 0)^T$, which is a column vector of length tm. It follows from Theorem 5 that $\mathsf{C_f} = \overline{(\mathsf{C}_\mathbf{f}^*)^\perp}^\perp$ and $\dim(\mathsf{C_f}) = \dim(\overline{\mathsf{C}_\mathbf{f}^*})+1$.

Finally, we are in a position to prove the last conclusion. We first prove that $\sum_{x\in \mathrm{GF}(q^m)^*} x^j = 0$ for each j with $1 \le j \le q^m-2$. Let $i=\gcd(j, q^m-1)$. Set $\beta = \alpha^i$. Then $\beta^{(q^m-1)/i}=1$. Consequently,

$$\sum_{x\in \mathrm{GF}(q^m)^*} x^j = \sum_{x\in \mathrm{GF}(q^m)^*} x^i = \sum_{\ell=0}^{q^m-2} \alpha^{ij} = i \sum_{\ell=0}^{\frac{q^m-1}{i}-1} \beta^\ell = 0.$$

It then follows from $f_i(0)=0$ that

$$\sum_{x\in \mathrm{GF}(q^m)^*} f_i(x) = 0.$$

As a result, $\overline{\mathsf{C}_\mathbf{f}^*}$ has the generator matrix

$$\left[\, G\, \mathbf{0} \,\right].$$

The last desired conclusion then follows. Notice that $\overline{\mathsf{C}_\mathbf{f}^*}$ is a trivial extension.

When each f_i is a monomial, the codes $\mathsf{C}_\mathbf{f}^*$ and $(\mathsf{C}_\mathbf{f}^*)^\perp$ are cyclic, and $\mathsf{C_f}$ is the dual of an extended cyclic code by Theorem 6. In general, $\mathsf{C}_\mathbf{f}^*$ and $(\mathsf{C}_\mathbf{f}^*)^\perp$ may not be cyclic, and $\mathsf{C_f}$ is not an extended cyclic code. The code $\mathsf{C_f}$ is obtained from $\mathsf{C}_\mathbf{f}^*$ in the following order:

$$\mathsf{C}_\mathbf{f}^* \longrightarrow (\mathsf{C}_\mathbf{f}^*)^\perp \longrightarrow \overline{(\mathsf{C}_\mathbf{f}^*)^\perp} \longrightarrow \overline{(\mathsf{C}_\mathbf{f}^*)^\perp}^\perp = \mathsf{C_f}.$$

Let the coordinates of the code $\mathsf{C_f}$ be indexed by the elements in the ordered set $\mathrm{GF}(q^m)$. Any $\sigma_{(u,v)}(y) = uy+v \in \mathrm{GA}_1(\mathrm{GF}(q^m))$ maps $\mathsf{C_f}$ into the following code

$$\left\{ \left(\mathrm{Tr}\left(\sum_{i=1}^t a_i f_i(ux+v) \right) + h \right)_{x\in \mathrm{GF}(q^m)} : a_i \in \mathrm{GF}(q^m),\ h\in \mathrm{GF}(q) \right\}.$$

In general, the code $\mathsf{C_f}$ may not be affine-invariant. In some special cases, $\mathsf{C_f}$ is affine-invariant.

Let $t\ge 2$ be an integer. For any set of integers $\{i_2, \cdots, i_t\}$ with $0 \le i_2 < \cdots < i_t \le \lfloor m/2 \rfloor$, we consider the following code

$$\mathsf{C}(1, i_2, \cdots, i_t) = \{\mathbf{c}_{(h,a_1,\ldots,a_t)} : h\in \mathrm{GF}(q),\ a_i \in \mathrm{GF}(q^m)\} \tag{6}$$

where

$$\mathbf{c}_{(h,a_1,\ldots,a_t)} = \left(h + \mathrm{Tr}\left(a_1 x + \sum_{\ell=2}^t a_\ell x^{1+q^{i_\ell}} \right) \right)_{x\in \mathrm{GF}(q^m)}. \tag{7}$$

We now prove that $\mathsf{C}(1, i_2, \cdots, i_t)$ and its dual are affine-invariant and hold support 2-designs.

Theorem 7 *The code $\mathsf{C}(1, i_2, \cdots, i_t)$ defined in (6) is affine-invariant and the supports of all codewords of any fixed weight in the code form a 2-design. The same conclusions hold for the dual code $\mathsf{C}(1, i_2, \cdots, i_t)^\perp$.*

Proof Define

$$f(x) = h + \mathrm{Tr}\left(a_1 x + \sum_{\ell=2}^{t} a_\ell x^{1+q^{i_\ell}}\right).$$

For $u \in \mathrm{GF}(q^m)^*$ and $v \in \mathrm{GF}(q^m)$, we have

$$\begin{aligned} f(ux+v) &= h + \mathrm{Tr}\left(a_1(ux+v) + \sum_{\ell=2}^{t} a_\ell (ux+v)^{1+q^{i_\ell}}\right) \\ &= h + \mathrm{Tr}\left(a_1 v + \sum_{\ell=2}^{t} a_\ell v^{1+q^{i_\ell}}\right) + \\ &\quad \mathrm{Tr}\left(u\left(a_1 + \sum_{\ell=2}^{t}\left[a_\ell v^{q^{i_\ell}} + (a_\ell v)^{q^{m-i_\ell}}\right]\right)x\right) + \mathrm{Tr}\left(\sum_{\ell=2}^{t} a_\ell u^{1+q^{i_\ell}} x^{1+q^{i_\ell}}\right). \qquad (8) \end{aligned}$$

Let $\sigma_{(u,v)}(x) = ux + v$, where $u \in \mathrm{GF}(q^m)^*$ and $v \in \mathrm{GF}(q^m)$. It then follows from (8) that

$$\sigma_{(u,v)}(\mathbf{c}_{(h,a_1,\ldots,a_t)}) = \mathbf{c}_{(h',a'_1,\ldots,a'_t)} \in \mathsf{C}(1, i_2, \ldots, i_t),$$

where

$$\begin{aligned} h' &= f(v), \\ a'_1 &= u\left(a_1 + \sum_{\ell=2}^{t}\left[a_\ell v^{q^{i_\ell}} + (a_\ell v)^{q^{m-i_\ell}}\right]\right), \\ a'_\ell &= a_\ell u^{1+q^{1+q^{i_\ell}}} \text{ for } 2 \le \ell \le t. \end{aligned}$$

Hence, $\mathsf{C}(1, i_2, \ldots, i_t)$ is affine-invariant. Since the group $\mathrm{GA}_1(\mathrm{GF}(q^m))$ acts on $\mathrm{GF}(q^m)$ doubly transitively, the conclusion on the support designs of $\mathsf{C}(1, i_2, \ldots, i_t)$ holds.

It is well known that the permutation automorphism groups of any code C and its dual are the same. The desired conclusions on $\mathsf{C}(1, i_2, \ldots, i_t)^\perp$ follow from those of $\mathsf{C}(1, i_2, \ldots, i_t)$.

It is easily seen that $\mathsf{C}(1, i_2, \ldots, i_t)$ is an extended cyclic code, as the permutation $\sigma(x) = \alpha x$ fixes the code. In fact, it is the extended code of the cyclic code over $\mathrm{GF}(q)$ with length $q^m - 1$ and check polynomial

$$h(x) = \mathrm{LCM}\left((x-1), \mathbb{M}_{\alpha^{-1}}(x), \mathbb{M}_{\alpha^{-(1+q^{i_2})}}(x), \cdots, \mathbb{M}_{\alpha^{-(1+q^{i_t})}}(x)\right),$$

where α is a generator of $\mathrm{GF}(q^m)$, $\mathbb{M}_{\alpha^\ell}(x)$ $(2 \le \ell \le t)$ denotes the minimal polynomial of α^ℓ over $\mathrm{GF}(q)$, and LCM denotes the least common multiple of the polynomials. The dimension of the code $\mathsf{C}(1, i_2, \ldots, i_t)$ in Theorem 7 depends on the degree of the polynomial $h(x)$. The weight distribution of the code $\mathsf{C}(1, i_2, \ldots, i_t)$ is known in some special cases. The determination of the parameters of the support designs of the codes $\mathsf{C}(1, i_2, \ldots, i_t)$ and $\mathsf{C}(1, i_2, \ldots, i_t)^\perp$ is difficult in general, but can be done in some special cases.

Theorem 7 says that the code $\mathsf{C}(1, i_2, \ldots, i_t)$ and its dual hold 2-designs. It will be soon demonstrated below that the two codes hold 3-designs in some special cases.

3.1 The special case $q = 2$

When $q = 2$, the codes $\mathsf{C}(1, i_2, \ldots, i_t)$ and $\mathsf{C}(1, i_2, \ldots, i_t)^\perp$ become the affine-invariant binary codes treated in [12], where a class of Steiner systems $S(2, 4, 2^m)$ was obtained. Notice that these codes were treated as extended cyclic codes in [12].

3.2 Several special cases of 3-designs

In this section, we show a few cases in which $\mathsf{C}(1,i_2,\ldots,i_t)$ and its dual hold 3-designs. The results presented in this section are from [13].

Theorem 8 . *Let $m \geq 5$ and $(i_2,i_3)=(1,2)$ or $(i_2,i_3)=(1,(m+1)/2)$. Then the code $\mathsf{C}(1,i_2,i_3)$ has parameters $[2^m, 3m+1, 2^{m-1}-2^{(m+1)/2}]$ and weight enumerator*

$$A(z) = 1+uz^{2^{m-1}-2^{\frac{m+1}{2}}}+vz^{2^{m-1}-2^{\frac{m-1}{2}}}+wz^{2^{m-1}}+vz^{2^{m-1}+2^{\frac{m-1}{2}}}+uz^{2^{m-1}+2^{\frac{m+1}{2}}}+z^{2^m}, \tag{9}$$

where

$$\begin{aligned} u &= \frac{2^{3m-4}-3\times 2^{2m-4}+2^{m-3}}{3}, \\ v &= \frac{5\times 2^{3m-2}+3\times 2^{2m-2}-2^{m+1}}{3}, \\ w &= 2(2^m-1)(9\times 2^{2m-4}+3\times 2^{m-3}+1). \end{aligned}$$

The dual code $\mathsf{C}(1,i_2,i_3)^{\perp}$ has parameters $[2^m, 2^m-1-3m, 8]$, and its weight distribution is given by

$$2^{3m+1}A_k^{\perp} = \left(1+(-1)^k\right)\binom{2^m}{k}+wE_0(k)+uE_1(k)+vE_2(k), \tag{10}$$

where

$$E_0(k) = \frac{1+(-1)^k}{2}(-1)^{\lfloor k/2\rfloor}\binom{2^{m-1}}{\lfloor k/2\rfloor},$$

$$E_1(k) = \sum_{\substack{0\leq i\leq 2^{m-1}-2^{(m+1)/2} \\ 0\leq j\leq 2^{m-1}+2^{(m+1)/2} \\ i+j=k}} [(-1)^i+(-1)^j]\binom{2^{m-1}-2^{(m+1)/2}}{i}\binom{2^{m-1}+2^{(m+1)/2}}{j},$$

$$E_2(k) = \sum_{\substack{0\leq i\leq 2^{m-1}-2^{(m-1)/2} \\ 0\leq j\leq 2^{m-1}+2^{(m-1)/2} \\ i+j=k}} [(-1)^i+(-1)^j]\binom{2^{m-1}-2^{(m-1)/2}}{i}\binom{2^{m-1}+2^{(m-1)/2}}{j},$$

where $0\leq k\leq 2^m$.

The 3-designs held in $\mathsf{C}(1,i_2,i_3)$ and its dual are documented below.

Theorem 9 *Let $m\geq 5$ be an odd integer and $(i_2,i_3)=(1,2)$ or $(i_2,i_3)=(1,(m+1)/2)$. Let $\mathcal{P}=\{0,1,2,\cdots,2^m-1\}$, and let $\mathcal{B}_k$ be the set of the supports of the codewords of $\mathsf{C}(1,i_2,i_3)$ with weight k, where $A_k\neq 0$. Then $(\mathcal{P},\mathcal{B}_k)$ is a 3-$(2^m,k,\lambda)$ design, where*

$$\lambda = \frac{A_k\binom{k}{3}}{\binom{2^m}{3}},$$

where A_k is given in Theorem 8.

Let $\mathcal{P} = \{0,1,2,\cdots,2^m-1\}$, and let $\mathcal{B}_k^\perp$ be the set of the supports of the codewords of $\mathsf{C}(1,i_2,i_3)^\perp$ with weight k and $A_k^\perp \neq 0$. Then $(\mathcal{P},\mathcal{B}_k^\perp)$ is a 3-$(2^m,k,\lambda^\perp)$ design, where

$$\lambda^\perp = \frac{A_k^\perp \binom{k}{3}}{\binom{2^m}{3}},$$

where $A_k^\perp$ is given in Theorem 8.

Experimental data shows that the support 3-designs in Theorem 9 are not 4-designs. So far, no infinite family of 4-designs has been directly constructed from nonlinear or linear codes in the literature. The following is an important question in combinatorics and coding theory.

Open Problem 1 *Is there a special family of codes $\mathsf{C}(1,i_2,\ldots,i_t)$ holding 4-designs?*

3.3 Other cases

Other recent developments can be found in [17–19], where the designs are from affine-invariant codes that are derived from special functions.

4 Designs from almost bent functions

For any function g from GF(2^m) to GF(2^m), we define

$$\lambda_g(a,b) = \sum_{x\in \mathrm{GF}(2^m)} (-1)^{\mathrm{Tr}_{2^m/2}(ag(x)+bx)}, \ a, b \in \mathrm{GF}(2^m).$$

A function g from GF(2^m) to GF(2^m) is called *almost bent* if $\lambda_g(a,b) = 0, \text{ or } \pm 2^{(m+1)/2}$ for every pair (a,b) with $a \neq 0$. By definition, almost bent functions over GF(2^m) exist only for odd m.

The following is a list of almost bent functions on GF(2^m), where m is odd.

1. $g(x) = x^{2^i+1}$, $\gcd(i,m) = 1$.
2. $g(x) = x^{2^{2i}-2^i+1}$, $\gcd(i,m) = 1$.
3. $g(x) = x^{2^{(m-1)/2}+3}$.
4. $g(x) = x^{2^{(m-1)/2}+2^{(m-1)/4}-1}$, $m \equiv 1 \pmod 4$.
5. $g(x) = x^{2^{(m-1)/2}+2^{(3m-1)/4}-1}$, $m \equiv 3 \pmod 4$.
6. $g(x) = x^{2^i+1} + (x^{2^i}+x)\mathrm{Tr}_{2^m/2}(x^{2^i+1}+x)$, $m > 3$ and $\gcd(i,m) = 1$.

More known families of almost bent functions can be found in [31].

For any function g from GF(2^m) to GF(2^m) with $g(0) = 0$, we define the following linear code

$$\mathsf{C}_g = \{\left(\mathrm{Tr}_{2^m/2}(ag(x)+bx)+h\right)_{x\in\mathrm{GF}(2^m)}, \ a, b \in \mathrm{GF}(2^m), h \in \mathrm{GF}(2)\}. \qquad (11)$$

Theorem 10 *Let $m \geq 5$. The code C_g of (11) has parameters $[2^m, 2m+1, 2^{m-1}-2^{(m-1)/2}]$ and weight enumerator*

$$A(z) = 1 + uz^{2^{m-1}-2^{(m-1)/2}} + vz^{2^{m-1}} + uz^{2^{m-1}+2^{(m-1)/2}} + z^{2^m}, \qquad (12)$$

where

$$u = 2^{2m-1} - 2^{m-1} \text{ and } v = 2^{2m} + 2^m - 2.$$

The dual code $\mathsf{C}_g^\perp$ *has parameters* $[2^m, 2^m - m - 1, 6]$ *and its weight distribution is given by*

$$\begin{aligned} 2^{2m+1} A_k^\perp = {} & (1 + (-1)^k)\binom{2^m}{k} + \frac{1+(-1)^k}{2}(-1)^{\lfloor k/2 \rfloor}\binom{2^{m-1}}{\lfloor k/2 \rfloor} v + \\ & u \sum_{\substack{0 \le i \le 2^{m-1} - 2^{\frac{m-1}{2}} \\ 0 \le j \le 2^{m-1} + 2^{\frac{m-1}{2}} \\ i+j=k}} [(-1)^i + (-1)^j] \binom{2^{m-1} - 2^{\frac{m-1}{2}}}{i} \binom{2^{m-1} + 2^{\frac{m-1}{2}}}{j} \end{aligned}$$

for $0 \le k \le 2^m$.

The parameters and weight enumerator of the code C_g were stated specifically in [35]. The conclusions on the dual code $\mathsf{C}_g^\perp$ were proved in [15]. It is open who first studied the code C_g. But related cyclic codes were studied in [2,3,8].

The following theorem follows from Theorem 10 and the Assmus-Mattson Theorem (see [15]).

Theorem 11 *Let* $m \ge 5$ *be odd. Let* $\mathcal{P} = \{0, 1, 2, \cdots, 2^m - 1\}$, *and let* $\mathcal{B}_k$ *be the set of the supports of the codewords of* C_g *with weight k, where* $A_k \neq 0$. *Then* $(\mathcal{P}, \mathcal{B}_k)$ *is a* 3-$(2^m, k, \lambda)$ *design, where*

$$\lambda = \frac{A_k \binom{k}{3}}{\binom{2^m}{3}},$$

and A_k *is given in (12).*

Let $\mathcal{P} = \{0, 1, 2, \cdots, 2^m - 1\}$, *and let* $\mathcal{B}_k^\perp$ *be the set of the supports of the codewords of* $\mathsf{C}_g^\perp$ *with weight k and* $A_k^\perp \neq 0$. *Then* $(\mathcal{P}, \mathcal{B}_k^\perp)$ *is a* 3-$(2^m, k, \lambda^\perp)$ *design, where*

$$\lambda^\perp = \frac{A_k^\perp \binom{k}{3}}{\binom{2^m}{3}},$$

and $A_k^\perp$ *is given in Theorem 10.*

As shown above, every almost bent function on GF(2^m) yields two families of 3-designs. Hence, this is a general construction of 3-designs. The designs from almost bent monomials were pointed out in [15], where the codes C_g were treated as the extended codes of the corresponding cyclic codes. The treatment here is more general, as the designs from all almost bent functions are included.

Conjecture 12 *The code* C_g *of Theorem 10 is spanned by its minimum weight codes.*

5 Designs from planar functions

Throughout this section, let q be an odd prime. A function f from $\mathrm{GF}(q^m)$ to itself is called a *planar function* if the difference function $f_a(x) = f(x+a) - f(x)$ is a one-to-one function from $\mathrm{GF}(q^m)$ to itself for every $a \in \mathrm{GF}(q^m)^*$.

The following is a list of planar functions on $\mathrm{GF}(q^m)$:

1. $f(x) = x^2$.
2. $f(x) = x^{q^k+1}$, where $m/\gcd(m,k)$ is odd (Dembowski-Ostrom).
3. $f(x) = x^{(3^k+1)/2}$, where $q = 3$, k is odd, and $\gcd(m,k) = 1$ (Coulter-Matthews).
4. $f_u(x) = x^{10} - ux^6 - u^2x^2$, where $q = 3$, m is odd, and $u \in \mathrm{GF}(3^m)$ (Coulter-Matthews-Ding-Yuan).

More planar functions could be found in [31,30].

For any planar function f from $\mathrm{GF}(q^m)$ to $\mathrm{GF}(q^m)$ with $f(0) = 0$, define the following linear code

$$\mathsf{C}_f = \{ \left(\mathrm{Tr}_{q^m/q}(af(x) + bx) + h\right)_{x\in\mathrm{GF}(q^m)},\ a,\, b \in \mathrm{GF}(q^m), h \in \mathrm{GF}(q)\}. \tag{13}$$

The code C_f from specific planar functions was studied in [4] and [36]. The related subcode was investigated also in [20]. There is no general formula for the weight enumerator of C_f from planar functions. Hence, we have to treat the support designs of the codes C_f for specific families of planar functions.

Theorem 13 *Let $m \geq 3$ be odd. Let $f(x)$ be the Coulter-Matthews or a Coulter-Matthews-Ding-Yuan planar function on* $\mathrm{GF}(3^m)$*. Then C_f has parameters* $[3^m, 2m+1, 2\times 3^{m-1} - 3^{(m-1)/2}]$ *and weight enumerator*

$$1 + (q^m-1)q^m z^{(q-1)q^{m-1}-q^{(m-1)/2}} + ((q-2)q^{2m} + 2q^m - q)z^{(q-1)q^{m-1}} + \\ (q^m-1)q^m z^{(q-1)q^{m-1}+q^{(m-1)/2}} + (q-1)z^{q^m}, \tag{14}$$

where $q = 3$. The dual code $\mathsf{C}_f^\perp$ has minimum distance 5. The code C_f holds a support 2-design for each nonzero weight.

Proof The desired weight distribution can be proved by refining the proofs of Theorems 18 and 14 in [36]. The desired conclusion on the minimum distance of $\mathsf{C}_f^\perp$ was proved in [4]. The last desired conclusion follows from the Assmus-Mattson Theorem.

The parameters of the support 2-designs of the code C_f in Theorem 13 can be worked out. The details are left to the reader. The dual code $\mathsf{C}_f^\perp$ holds also 2-designs.

Theorem 14 *Let $m \geq 3$ be an integer. Let $f(x)$ be x^2 or the Dembowski-Ostrom planar function on* $\mathrm{GF}(q^m)$*. Then C_f and $\mathsf{C}_f^\perp$ hold a support 2-design for every nonzero weight.*

Proof It follows from Theorem 7.

It was proved in [4] that the code $\mathsf{C}_f^\perp$ in Theorem 14 has minimum distance 4 if $q > 3$ and 5 if $q = 3$. When m is odd, the code C_f in Theorem 14 has the weight enumerator in (14). When m is even, C_f has six nonzero weights. The parameters of the support 2-designs of the code C_f in Theorem 14 could be settled. The details are left to the reader.

We remark that the classical codes $\mathsf{C}_q(\mathbb{D})$ of the support designs $\mathbb{D}$ in Theorems 13 and 14 are very different from the original codes C_f. For example, when $(m,q) = (3,3)$ and $f(x) = x^2$, the code C_f has parameters $[27,7,15]$, and $\mathsf{C}_3(\mathbb{D})$ has parameters $[27,19,6]$, which is optimal. It would be interesting to study these codes $\mathsf{C}_q(\mathbb{D})$.

6 Designs from bent vectorial functions

A symmetric 2-design is said to have the *symmetric difference property*, or to be a *symmetric SDP design*, if the symmetric difference of any *three* blocks is either a block or the complement of a block. Kantor introduced and demonstrated a lot of symmetric SDP designs [24, 25]. It is known that any symmetric SDP design has the following parameters

$$(2^m, 2^{m-1} \pm 2^{(m-2)/2}, 2^{m-2} \pm 2^{(m-2)/2}) \tag{15}$$

for some positive integer m. Dillion and Schatz proved that each symmetric SDP design is a support design of a linear code of length 2^m from a bent function on $\mathrm{GF}(2^m)$ [9]. Recently, the construction of Dillion and Schatz was generalized by using bent vectorial functions in [16]. The objective of this section is to introduce this generalised construction in [16].

6.1 Bent vectorial functions

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

An (m, ℓ) vectorial Boolean function $F(x) = (f_1(x), \cdots, f_\ell(x))$ is called a *bent vectorial function* if $\sum_{j=1}^{\ell} a_j f_j(x)$ is a bent function for each nonzero $(a_1, \cdots, a_\ell) \in \mathrm{GF}(2)^\ell$. For another equivalent definition of bent vectorial functions, see [30, Chapter 12].

Bent vectorial functions exist only when $\ell \leq m/2$ (cf. [30, Chapter 12]). There are a number of known constructions of bent vectorial functions. The reader is referred to [5] and [30, Chapter 12] for detailed information. Below we present a specific construction of bent vectorial functions from [5].

Example 1 [5]. Let $m/2 \geq 1$ be an odd integer, $\beta_1, \beta_2, \cdots, \beta_{m/2}$ be a basis of $\mathrm{GF}(2^{m/2})$ over $\mathrm{GF}(2)$, and let $u \in \mathrm{GF}(2^m) \setminus \mathrm{GF}(2^{m/2})$. Let i be a positive integer with $\gcd(m, i) = 1$. Then

$$\left(\mathrm{Tr}_{2^m/2}(\beta_1 u x^{2^i+1}), \mathrm{Tr}_{2^m/2}(\beta_2 u x^{2^i+1}), \cdots, \mathrm{Tr}_{2^m/2}(\beta_{m/2} u x^{2^i+1})\right) \tag{16}$$

is an $(m, m/2)$ bent vectorial function.

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

It is known that a function F from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2^\ell)$ is bent if and only if $\mathrm{Tr}_{2^\ell/2}(aF(x))$ is a bent Boolean function for all $a \in \mathrm{GF}(2^\ell)^*$. Any such vectorial function F can be expressed as $\mathrm{Tr}_{2^m/2^\ell}(f(x))$, 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 2 (cf. [30, Chapter 12]). Let $m/2 > 1$ and $i \geq 1$ be integers such that $m/\gcd(i, m)$ is even. Then $\mathrm{Tr}_{2^m/2^{m/2}}(ax^{2^i+1})$ is bent if and only if $\gcd(2^i+1, 2^{m/2}+1) \neq 1$ and $a \in \mathrm{GF}(2^m)^* \setminus \langle \alpha^{\gcd(2^i+1, 2^{m/2}+1)} \rangle$, where α is a generator of $\mathrm{GF}(2^m)^*$.

Example 3 (cf. [30, Chapter 12]). Let $m/2 > 1$ and $i \geq 1$ be integers such that $\gcd(i, m) = 1$. Let $d = 2^{2i} - 2^i + 1$. Let $m/2$ be odd. Then $\mathrm{Tr}_{2^m/2^{m/2}}(ax^d)$ is bent if and only if $a \in \mathrm{GF}(2^m)^* \setminus \langle \alpha^3 \rangle$, where α is a generator of $\mathrm{GF}(2^m)^*$.

6.2 A construction of binary codes from bent vectorial functions

Let m be even and $r = 2^m$. Let $\mathrm{GF}(r) = \{u_1, u_2, \cdots, u_r\}$, and let w be a generator of $\mathrm{GF}(r)^*$. We use the following generator matrix of the binary $[2^m, m+1, 2^{m-1}]$ first-order Reed-Muller code $\mathrm{RM}_2(1,m)$:

$$G_0 = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \mathrm{Tr}_{2^m/2}(w^0 u_1) & \mathrm{Tr}_{2^m/2}(w^0 u_2) & \cdots & \mathrm{Tr}_{2^m/2}(w^0 u_r) \\ \vdots & \vdots & \ddots & \vdots \\ \mathrm{Tr}_{2^m/2}(w^{m-1} u_1) & \mathrm{Tr}_{2^m/2}(w^{m-1} u_2) & \cdots & \mathrm{Tr}_{2^m/2}(w^{m-1} u_r) \end{bmatrix}. \qquad (17)$$

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

$$1 + (2^{m+1} - 2) z^{2^{m-1}} + z^{2^m}. \qquad (18)$$

Up to equivalence, $\mathrm{RM}_2(1,m)$ is the unique linear binary code with parameters $[2^m, m+1, 2^{m-1}]$. Its dual code is the $[2^m, 2^m - 1 - m, 4]$ Reed-Muller code of order $m-2$. Both codes hold 3-designs since they are invariant under a 3-transitive affine group. Note that $\mathrm{RM}_2(1,m)^\perp$ 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 $F(x) = (f_1(x), f_2(x), \cdots, f_\ell(x))$ be an (m,ℓ) vectorial function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)^\ell$. For each i, $1 \le i \le \ell$, we define a binary vector

$$F_i = (f_i(u_1), f_i(u_2), \cdots, f_i(u_r)) \in \mathrm{GF}(2)^{2^m}, \qquad (19)$$

which is the truth table of the Boolean function $f_i(x)$.

Let ℓ be an integer in the range $1 \le \ell \le m/2$. We now define an $(m+1+\ell) \times 2^m$ matrix

$$G = G(f_1, \cdots, f_\ell) = \begin{bmatrix} G_0 \\ F_1 \\ \vdots \\ F_\ell \end{bmatrix}, \qquad (20)$$

where G_0 is the generator matrix of $\mathrm{RM}_2(1,m)$. Let $\mathsf{C}(f_1, \cdots, f_\ell)$ denote the binary code of length 2^m with generator matrix $G(f_1, \cdots, f_\ell)$ given by (20). The dimension of the code has the following lower and upper bounds:

$$m + 1 \le \dim(\mathsf{C}(f_1, \cdots, f_\ell)) \le m + 1 + \ell.$$

The next theorem gives a coding-theoretical characterization of bent vectorial functions. In the case $\ell = 1$, it gives a coding-theoretical characterization of bent functions.

Theorem 15 *An (m,ℓ) vectorial function $F(x) = (f_1(x), f_2(x), \cdots, f_\ell(x))$ from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)^\ell$ is a bent vectorial function if and only if the code $\mathsf{C}(f_1, \cdots, f_\ell)$ with generator matrix G given by (20) has weight enumerator*

$$1 + (2^\ell - 1) 2^m z^{2^{m-1} - 2^{(m-2)/2}} + 2(2^m - 1) z^{2^{m-1}} + (2^\ell - 1) 2^m z^{2^{m-1} + 2^{(m-2)/2}} + z^{2^m}. \qquad (21)$$

Theorem 16 *The code $\mathsf{C} = \mathsf{C}(f_1, \cdots, f_\ell)$ from Theorem 17 is spanned by the set of codewords of minimum weight.*

6.3 A construction of 2-designs from bent vectorial functions

The following theorem documents the support designs of the code $\mathsf{C} = \mathsf{C}(f_1, \cdots, f_\ell)$ from a bent vectorial function.

Theorem 17 *Let $F(x) = (f_1(x), f_2(x), \cdots, f_\ell(x))$ be a bent vectorial function from* $\mathrm{GF}(2^m)$ *to* $\mathrm{GF}(2)^\ell$*, where $m/2 \geq 2$ and $1 \leq \ell \leq m/2$. Let $\mathsf{C} = \mathsf{C}(f_1, \cdots, f_\ell)$ be the binary linear code with parameters $[2^m, m+1+\ell, 2^{m-1} - 2^{(m-2)/2}]$ defined in Theorem 15.*
(a) The codewords of C of minimum weight hold a 2-design $\mathbb{D}$ with parameters

$$2-(2^m, 2^{m-1} - 2^{(m-2)/2}, (2^\ell - 1)(2^{m-2} - 2^{(m-2)/2})). \tag{22}$$

Further, $\mathsf{C}_2(\mathbb{D})$ is equal to C.
(b) The codewords of C of weight $2^{m-1} + 2^{(m-2)/2}$ hold a 2-design $\overline{\mathbb{D}}$ with parameters

$$2-(2^m, 2^{m-1} + 2^{(m-2)/2}, (2^\ell - 1)(2^{m-2} + 2^{(m-2)/2})). \tag{23}$$

Further, $\mathsf{C}_2(\overline{\mathbb{D}})$ equals C.

We remark that Theorem 17 cannot be proved by the Assmus-Mattson Theorem or the automorphism group of the code C. It is clear that the supports of all codewords of weight 2^{m-1} in the code $\mathsf{C}(f_1, \cdots, f_\ell)$ of Theorem 17 form a 2-design. It then follows from Theorem 3 that the supports of all codewords of any fixed nonzero weight in the dual code $\mathsf{C}(f_1, \cdots, f_\ell)^\perp$ form a 2-design. The weight distribution of $\mathsf{C}(f_1, \cdots, f_\ell)^\perp$ can be obtained via Theorem 4.

The special case $\ell = 1$ Theorem 17 implies as a corollary the following result of Dillon and Schatz [9].

Theorem 18 *Let $f(x)$ be a bent function from* $\mathrm{GF}(2^m)$ *to* $\mathrm{GF}(2)$*. Then the code $\mathsf{C}(f)$ has parameters $[2^m, m+2, 2^{m-1} - 2^{(m-2)/2}]$ and weight enumerator*

$$1 + 2^m z^{2^{m-1} - 2^{(m-2)/2}} + 2(2^m - 1) z^{2^{m-1}} + 2^m z^{2^{m-1} + 2^{(m-2)/2}} + z^{2^m}. \tag{24}$$

The minimum weight codewords form a symmetric SDP design with parameters

$$2-(2^m, 2^{m-1} - 2^{(m-2)/2}, 2^{m-2} - 2^{(m-2)/2}). \tag{25}$$

Dillion and Schatz showed that every symmetric SDP design with the parameters of (25) is a support design of $\mathsf{C}(f)$ for some bent function f from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ [9].

Corollary 1 *Two codes $\mathsf{C}_f = \mathsf{C}(f_1, \cdots, f_s)$, $\mathsf{C}_g = \mathsf{C}(g_1, \cdots, g_s)$ obtained from bent vectorial functions $(f_1, \cdots, f_s)$, $(g_1, \cdots, g_s)$ are equivalent if and only if the designs supported by their minimum weight vectors are isomorphic.*

By Theorem 18, the codes based on single bent functions support symmetric 2-designs. The next theorem determines the block intersection numbers of the design $\mathbb{D}(f_1, \cdots, f_\ell)$ supported by the minimum weight vectors in the code $\mathsf{C}(f_1, \cdots, f_\ell)$ from Theorem 17.

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

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

supported by the minimum weight codewords of a code $\mathsf{C} = \mathsf{C}(f_1, \ldots, f_\ell)$ defined as in Theorem 17.

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

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

$$s_1 = 2^{m-2} - 2^{(m-4)/2},\ s_2 = 2^{m-2} - 2^{(m-2)/2},\ s_3 = 2^{m-2} - 3 \cdot 2^{(m-4)/2}. \tag{26}$$

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

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

7 Quasisymmetric designs from bent functions

A 2-design is *quasi-symmetric* with intersection numbers x and y if any two distinct blocks intersect in either x and y points. A nonsymmetric 2-design is said to have the *symmetric difference property*, or to be an *SDP design*, if the symmetric difference of any *two* blocks is either a block or the complement of a block. In this section, we present a construction of all quasisymmetric designs from bent functions. This is also a coding-theoretic construction of designs.

7.1 A general construction of linear codes with bent functions

Let f be a Boolean function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$, and let D_f be the support of f. Denote $D_f = \{d_1, d_2, \ldots, d_{n_f}\} \subseteq \mathrm{GF}(2^m)$. Let Tr denote the trace function from $\mathrm{GF}(2^m)$ onto $\mathrm{GF}(2)$ throughout this section. We define a binary linear code of length n_f by

$$\mathsf{C}_{D_f} = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_{n_f})) : x \in \mathrm{GF}(2^m)\}, \tag{28}$$

and call D_f the *defining set* of this code C_{D_f}. This is a special case of a general construction of linear codes, which has been intensively and extensively investigated recently [11].

A proof of the following theorem can be found in [10]. The construction of the codes with bent functions is euqivalent to that of [34].

Table 1 The weight distribution of the codes of Theorem 20

Weight w	Multiplicity A_w
0	1
$\frac{n_f}{2} - 2^{\frac{m-4}{2}}$	$\frac{2^m - 1 - n_f 2^{-\frac{m-2}{2}}}{2}$
$\frac{n_f}{2} + 2^{\frac{m-4}{2}}$	$\frac{2^m - 1 + n_f 2^{-\frac{m-2}{2}}}{2}$

Theorem 20 *Let f be a bent function from* $\mathrm{GF}(2^m)$ *to* $\mathrm{GF}(2)$*, where $m \geq 4$ and is even. Then C_{D_f} is an* $[n_f, m, (n_f - 2^{(m-2)/2})/2]$ *two-weight binary code with the weight distribution in Table 1, where n_f is defined in (3).*

It is easy to see that the dual code $\mathsf{C}_{D_f}^{\perp}$ has minimum distance at least 3. Unfortunately, the code C_{D_f} and its dual $\mathsf{C}_{D_f}^{\perp}$ do not hold 2-designs. However, it was observed in [14, Chapter 14] that their augmented codes hold infinite families of 2-designs.

Let f be a bent function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$, and let D_f be the support of f. Denote $D_f = \{d_1, d_2, \ldots, d_{n_f}\} \subseteq \mathrm{GF}(2^m)$. We define a binary linear code of length n_f by

$$\tilde{\mathsf{C}}_{D_f} = \{(\mathrm{Tr}(xd_1), \mathrm{Tr}(xd_2), \ldots, \mathrm{Tr}(xd_{n_f})) + y\mathbf{1} : x \in \mathrm{GF}(2^m), y \in \mathrm{GF}(2)\}, \tag{29}$$

where $\mathbf{1}$ denote the vector $(1, 1, \cdots, 1) \in \mathrm{GF}(2)^{n_f}$. This code $\tilde{\mathsf{C}}_{D_f}$ is the augmented code of C_{D_f}.

Table 2 The weight distribution of the codes of Theorem 21

Weight w	Multiplicity A_w
0	1
$\frac{n_f}{2} - 2^{\frac{m-4}{2}}$	$2^m - 1$
$\frac{n_f}{2} + 2^{\frac{m-4}{2}}$	$2^m - 1$
n_f	1

Theorem 21 *Let f be a bent function from* $\mathrm{GF}(2^m)$ *to* $\mathrm{GF}(2)$*, where $m \geq 6$ and is even. Then $\tilde{\mathsf{C}}_{D_f}$ is an* $[n_f, m+1, (n_f - 2^{(m-2)/2})/2]$ *three-weight binary code with the weight distribution in Table 2, where n_f is defined in (3).*

Notice that the code $\tilde{\mathsf{C}}_{D_f}$ meets the Grey-Rankin bound, and is optimal. This shows the importance of bent functions in coding theory. The next theorem was proved in [14, Chapter 14].

Theorem 22 *Let f be a bent function from* $\mathrm{GF}(2^m)$ *to* $\mathrm{GF}(2)$*, where $m \geq 6$ and is even. When $n_f = 2^{m-1} - 2^{(m-2)/2}$, the dual code $\tilde{\mathsf{C}}_{D_f}^{\perp}$ has parameters* $[2^{m-1} - 2^{(m-2)/2}, 2^{m-1} - 2^{(m-2)/2} - m - 1, 4]$ *and weight distribution*

$$A_{2\ell}^{\perp} = 2\binom{2^{m-1} - 2^{\frac{m-2}{2}}}{2\ell} + (2^m - 1) \sum_{\substack{i+j=\ell \\ 0 \leq i \leq 2^{m-2} - 2^{\frac{m-4}{2}} \\ 0 \leq j \leq 2^{\frac{m-4}{2}}}} (-1)^i 2 \binom{2^{m-2} - 2^{\frac{m-2}{2}}}{i} \binom{2^{\frac{m-2}{2}}}{2j} \tag{30}$$

for $2 \leq \ell \leq 2^{m-2} - 2^{(m-4)/2}$ and $A_i^{\perp} = 0$ for other i, where $A_i^{\perp}$ denotes the number of codewords of weight i in $\tilde{\mathsf{C}}_{D_f}^{\perp}$.

When $n_f = 2^{m-1} + 2^{(m-2)/2}$, $\tilde{\mathsf{C}}_{D_f}^{\perp}$ has parameters $[2^{m-1} + 2^{(m-2)/2}, 2^{m-1} + 2^{(m-2)/2} - m - 1, 4]$ *and weight distribution*

$$A_{2\ell}^{\perp} = 2\binom{2^{m-1} + 2^{\frac{m-2}{2}}}{2\ell} + (2^m - 1) \sum_{\substack{i+j=\ell \\ 0 \leq i \leq 2^{m-2} \\ 0 \leq j \leq 2^{\frac{m-4}{2}}}} (-1)^i 2 \binom{2^{m-2}}{i} \binom{2^{\frac{m-2}{2}}}{2j} \tag{31}$$

for $2 \leq \ell \leq 2^{m-2} + 2^{(m-4)/2}$ and $A_i^{\perp} = 0$ for other i.

7.2 Infinite families of 2-designs from bent functions

It is known that binary codes with the weight distribution of Table 2 and their duals hold 2-designs [32,29]. A proof of the next two theorems can be found in [14, Chapter 14].

Theorem 23 *Let f be a bent function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$, where $m \geq 6$ and is even. When*

$$n_f = 2^{m-1} - 2^{(m-2)/2},$$

the supports of codewords of weight $2^{m-2} - 2^{\frac{m-2}{2}}$ in the code $\tilde{\mathsf{C}}_{D_f}$ of Theorem 21 form a quasi-symmetric SDP design $\mathbb{D}$ with the following parameters:

$$2 - \left(2^{m-1} - 2^{\frac{m-2}{2}},\, 2^{m-2} - 2^{\frac{m-2}{2}},\, 2^{m-2} - 2^{\frac{m-2}{2}} - 1\right).$$

Further, the code $\mathsf{C}_2(\mathbb{D})$ is equal to $\tilde{\mathsf{C}}_{D_f}$.

When

$$n_f = 2^{m-1} + 2^{(m-2)/2},$$

the supports of codewords of weight 2^{m-2} in the code $\tilde{\mathsf{C}}_{D_f}$ of Theorem 21 form a quasi-symmetric SDP design $\mathbb{D}$ with the following parameters:

$$2 - \left(2^{m-1} + 2^{\frac{m-2}{2}},\, 2^{m-2},\, 2^{m-2} - 2^{\frac{m-2}{2}}\right).$$

Further, the code $\mathsf{C}_2(\mathbb{D})$ is equal to $\tilde{\mathsf{C}}_{D_f}$.

It was shown in [14, Chapter 14] that every quasisymmetric SDP design is a support design of the code $\tilde{\mathsf{C}}_{D_f}$ for a suitable bent function f. This demonstrates the important of bent functions in combinatorial designs.

Theorem 24 *Let f be a bent function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$, where $m \geq 6$ and is even. When*

$$n_f = 2^{m-1} - 2^{(m-2)/2},$$

for each $2 \leq \ell \leq 2^{m-2} - 2^{(m-4)/2}$ with $A_{2\ell}^{\perp} \neq 0$, the supports of all codewords of weight 2ℓ in the code $\tilde{\mathsf{C}}_{D_f}^{\perp}$ form a 2-$(2^{m-1} - 2^{(m-2)/2},\, 2\ell, \lambda^{\perp})$ design, where

$$\lambda^{\perp} = \frac{A_{2\ell}^{\perp}\binom{2\ell}{2}}{\binom{2^{m-1}-2^{(m-2)/2}}{2}}$$

and $A_{2\ell}^{\perp}$ is given in (30).

When

$$n_f = 2^{m-1} + 2^{(m-2)/2},$$

for each $2 \leq \ell \leq 2^{m-2} + 2^{(m-4)/2}$ with $A_{2\ell}^{\perp} \neq 0$, the supports of all codewords of weight 2ℓ in the code $\tilde{\mathsf{C}}_{D_f}^{\perp}$ form a 2-$(2^{m-1} + 2^{(m-2)/2},\, 2\ell, \lambda^{\perp})$ design, where

$$\lambda^{\perp} = \frac{A_{2\ell}^{\perp}\binom{2\ell}{2}}{\binom{2^{m-1}+2^{(m-2)/2}}{2}}$$

and $A_{2\ell}^{\perp}$ is given in (31).

The next result was presented in [32].

Corollary 2 *Let f be a bent function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$, where $m \geq 6$ and is even. When*

$$n_f = 2^{m-1} - 2^{(m-2)/2},$$

the supports of all codewords of weight 4 in $\tilde{\mathsf{C}}_{D_f}^{\perp}$ form a 2-$(2^{m-1} - 2^{(m-2)/2},\ 4, \lambda^{\perp})$ design $\mathbb{D}$, where

$$\lambda^{\perp} = (2^{(m-4)/2} - 1)(2^{(m-2)/2} + 1).$$

Further, $\mathsf{C}_2(\mathbb{D})$ is equal to $\tilde{\mathsf{C}}_{D_f}^{\perp}$.

When

$$n_f = 2^{m-1} + 2^{(m-2)/2},$$

the supports of all codewords of weight 4 in $\tilde{\mathsf{C}}_{D_f}^{\perp}$ form a 2-$(2^{m-1} + 2^{(m-2)/2},\ 4, \lambda^{\perp})$ design $\mathbb{D}$, where

$$\lambda^{\perp} = (2^{(m-4)/2} + 1)(2^{(m-2)/2} - 1).$$

Further, $\mathsf{C}_2(\mathbb{D})$ is equal to $\tilde{\mathsf{C}}_{D_f}^{\perp}$.

The following was proved in [14, Chapter 14].

Corollary 3 *Let f be a bent function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$, where $m \geq 6$ and is even. When*

$$n_f = 2^{m-1} - 2^{(m-2)/2},$$

the supports of all codewords of weight 6 in $\tilde{\mathsf{C}}_{D_f}^{\perp}$ form a 2-$(2^{m-1} - 2^{(m-2)/2},\ 6, \lambda^{\perp})$ design, where

$$\lambda^{\perp} = \frac{1}{6}(2^{\frac{m-2}{2}} + 1)(2^{\frac{5m-10}{2}} - 3 \times 2^{2m-4} - 5 \times 2^{\frac{3m-8}{2}} + 25 \times 2^{m-3} + 2^{\frac{m}{2}} - 16).$$

When

$$n_f = 2^{m-1} + 2^{(m-2)/2},$$

the supports of all codewords of weight 6 in $\tilde{\mathsf{C}}_{D_f}^{\perp}$ form a 2-$(2^{m-1} + 2^{(m-2)/2},\ 6, \lambda^{\perp})$ design, where

$$\lambda^{\perp} = \frac{1}{6}(2^{\frac{m-2}{2}} - 1)(2^{\frac{5m-10}{2}} + 3 \times 2^{2m-4} - 5 \times 2^{\frac{3m-8}{2}} - 25 \times 2^{m-3} + 2^{\frac{m}{2}} + 16).$$

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

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

The b derived designs may be isomorphic or not. However, they have the same parameters. Consequently, we call them collectively the derived design. For the same reason, all the b residual designs are collectively called the residual design of $\mathbb{D}$.

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

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

its derived design has parameters

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

and its residual design has parameters

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

It is known that the quasisymmetric designs of Theorem 23 are derived designs of those symmetric designs of Theorem 18 [14, Chapter 14].

8 Designs from semibent functions on $\mathrm{GF}(2^m)$ for even m

Throughout this section, let $m \geq 4$ be even unless otherwise stated, and let $\mathrm{Tr}(x)$ denote the absolute trace function on $\mathrm{GF}(2^m)$. A function from $\mathrm{GF}(2^m)$ to $\mathrm{GF}(2)$ is called *semibent* if $\hat{f}(w) \in \{0, \pm 2^{(m+2)/2}\}$ for all $w \in \mathrm{GF}(2^m)$. We are much interested in semibent functions of the form $f(x) = \mathrm{Tr}(x^e)$. The following is list of such semibent functions $\mathrm{Tr}(x^e)$:

1. $e = 2^h + 1$, where $m/\gcd(m,h)$ is odd and $1 \leq h \leq m/2$ (Gold exponent) [21].
2. $e = 2^{2h} - 2^h + 1$, where $m/\gcd(m,h)$ is odd (Kasami exponent) ([26], [27]).
3. $e = 2^{m/2} + 2^{(m+2)/4} + 1$, where $m \equiv 2 \pmod 4$ (Niho exponent) [7].
4. $e = 2^{(m+2)/2} + 3$, where $m \equiv 2 \pmod 4$ (Niho exponent) [7].

In this section, we summarise semibent functions of the form $\mathrm{Tr}(x^e)$ that can be employed to obtain 2-designs in a way. To this end, we introduce two families of binary linear codes as follows.

Let e be an odd integer with $1 < e < 2^m - 1$ and $\gcd(e, 2^m - 1) = 1$. Assume that the smallest positive integer ℓ such that $2^\ell e \equiv e \pmod{2^m - 1}$ is m. Define

$$\mathsf{C}_e^* = \{(\mathrm{Tr}(ax^e + bx))_{x \in \mathrm{GF}(2^m)^*} : a, b \in \mathrm{GF}(2^m)\} \tag{32}$$

and

$$\mathsf{C}_e = \{(\mathrm{Tr}(ax^e + bx) + h)_{x \in \mathrm{GF}(2^m)} : a, b \in \mathrm{GF}(2^m),\ h \in \mathrm{GF}(2)\}. \tag{33}$$

By definition, C_e^* is isomorphic to the primitive cyclic code with parity-check polynomial $\mathbb{M}_{\alpha^{-e}}\mathbb{M}_{\alpha^{-1}}(x)$, where α is a generator of $\mathrm{GF}(2^m)^*$ and $\mathbb{M}_{\alpha^j}$ is the minimal polynomial of α^j over $\mathrm{GF}(2)$.

The parameters and the weight distribution of the code C_e^* are given in the next theorem.

Theorem 25 *Let notation and assumptions be as before. Then the code C_e^* has parameters $[2^m - 1, 2m]$ and its weight distribution is given by the following multiset union*

$$\begin{aligned}&\left\{\left\{(2^m - \hat{f}(w))/2 : w \in \mathrm{GF}(2^m), v \in \mathrm{GF}(2^m)^*\right\}\right\} \cup \\ &\left\{\left\{2^{m-1} : w \in \mathrm{GF}(2^m)^*\right\}\right\} \cup \{\{0\}\},\end{aligned}$$

where $f(x) = \mathrm{Tr}(x^e)$.

Proof Since $e > 1$ and e is odd, e and 1 are in different cyclotomic cosets modulo $2^m - 1$. By assumption, the cyclotomic coset containing e has size m. It then follows that the code C_e^* has dimension $2m$.

Since $\gcd(e, 2^m - 1) = 1$, y^e is a permutation of $\mathrm{GF}(2^m)$. Define

$$\mathbf{c}_{(a,b)} = (\mathrm{Tr}(ax^e + bx))_{x \in \mathrm{GF}(2^m)},\ a, b \in \mathrm{GF}(2^m).$$

Let $a \neq 0$. Then $ax^e = (a^{\frac{1}{e}}x)^e$. Consequently, $\mathbf{c}_{(a,b)}$ has the same Hamming weight as $\mathbf{c}_{(1, a^{-\frac{1}{e}}b)}$. Note that

$$\mathtt{wt}(\mathbf{c}_{(1, a^{-\frac{1}{e}}b)}) = \frac{2^m - \hat{f}(a^{-\frac{1}{e}}b)}{2}.$$

The desired conclusion on the weight distribution of the code then follows.

The following theorem follows from Theorem 25.

Theorem 26 *Let notation and assumptions be as before. Then the code* C_e *has parameters* $[2^m, 2m+1]$ *and its weight distribution is given by the following multiset union*

$$\left\{\left\{(2^m - \hat{f}(w))/2 : w \in \mathrm{GF}(2^m), v \in \mathrm{GF}(2^m)^*\right\}\right\} \cup$$
$$\left\{\left\{(2^m + \hat{f}(w))/2 : w \in \mathrm{GF}(2^m), v \in \mathrm{GF}(2^m)^*\right\}\right\} \cup$$
$$\left\{\left\{2^{m-1} : w \in \mathrm{GF}(2^m)^*, u \in \mathrm{GF}(2)\right\}\right\} \cup \{\{0\}\} \cup \{\{2^m\}\},$$

where $f(x) = \mathrm{Tr}(x^e)$.

We point out that Theorems 25 and 26 work for both even and odd m. In addition, Theorems 25 and 26 can be modified into more general results without restricting the size of the cyclotomic coset modulo $2^m - 1$ containing e.

Theorem 27 *Let e be the Gold, or Kasami or Niho exponent introduced before. Then the code* C_e *has parameters* $[2^m, 2m+1, 2^{m-1} - 2^{m/2}]$ *and weight enumerator*

$$1 + (2^m - 1)2^{m-2}z^{2^{m-1}-2^{m/2}} + (2^m - 1)(3 \times 2^{m-1} + 2)z^{2^{m-1}} + (2^m - 1)2^{m-2}z^{2^{m-1}+2^{m/2}} + z^{2^m}.$$

The dual code $\mathsf{C}_e^\perp$ *has parameters* $[2^m, 2^m - 2m - 1, 4]$.

Proof It is easily verified that $e > 1$ is odd and $\gcd(e, 2^m - 1) = 1$. Notice that $\mathrm{Tr}(x^e)$ is semibent. It then follows from Theorem 26 that the code C_e has the four nonzero weights given in the weight enumerator above. One can easily deduce that the dual code $(\mathsf{C}_e^*)^\perp$ has minimum weight at least 3. As a result, $\mathsf{C}_e^\perp$ has minimum distance at least 4. The first four Pless power moments then give the desired weight distribution of C_e. Using the MacWilliams identity and the weight enumerator of C_e, one can prove that the minimum distance of $\mathsf{C}_e^\perp$ equals 4.

The Assmus-Mattson Theorem says that the code C_e of Theorem 27 hold 1-designs. For the two Niho exonents e, C_e does not hold 2-designs according to Magma experiments. This means that the automorphism group of the code C_e for the two Niho exponents is in general not 2-homogeneous and 2-transitive.

Since $\mathrm{Tr}(x^{2^h+1})$ is a quadratic form, the code C_{2^h+1} is affine-invariant and holds 2-designs. Note that the Boolean function $\mathrm{Tr}(x^{2^{2h}-2^h+1})$ is not quadratic, and, in general, is not 2-transitive or 2-homogeneous. But our Magma program suggests the following conjecture.

Conjecture 28 *For the Kasami exponent* $e = 2^{2h} - 2^h + 1$*, the code* C_e *holds* 2*-designs.*

For any semibent function $\mathrm{Tr}(x^e)$, the code C_e and its dual $\mathsf{C}_e^\perp$ has the fixed parameters and weight enumerator in Theorem 27. However, some of these codes hold 2-designs, while others do not. This is due to the fact that the weight enumerator in Theorem 27 is not regular enough so that 2-designs are guaranteed.

9 Concluding remarks

In this survey, we summarized constructions of 2-designs and 3-designs held only in linear codes that are constructed with special types of functions. Special functions can also be employed to construct nonlinear codes which hold also designs. For example, the famous

Kerdock codes are nonlinear and are constructed with a set of bent functions such that the sum of any two of sum is still bent [28, Chapter 15].

As observed, the linear codes from special functions presented in this survey have very good parameters and some of them are optimal. It is very fascinating to search for special functions and their applications in coding theory and combinatorics. Hopefully, this survey could stimulate research in this direction.

References

1. Assmus Jr., E. F., Mattson Jr., H. F.: Coding and combinatorics, SIAM Rev. 16 (1974) 349–388.
2. Canteaut, C., Charpin, P., Dobbertin, H.: Weight divisibility of cyclic codes, highly nonlinear functions on F_{2^m}, and crosscorrelation of maximum-length sequences. SIAM J. Discret. Math. **13**, 105–138 (1998).
3. Carlet, C., Charpin, P., Zinoviev, V.: Codes, bent functions and permutations suitable for DES-like cryptosystems. Des. Codes Cryptogr. **15**, 125–126 (1998).
4. Carlet, C., Ding, C., Yuan, J.: Linear codes from perfect nonlinear mappings and their secret sharing schemes. IEEE Trans. Inf. Theory **51**, 2089–2102 (2005).
5. Carlet, C., Mesnager, S.: On the construction of bent vectorial functions. International Journal of Information and Coding Theory **1**, 133–148 (2010).
6. Carlet, C., Mesnager, S.: Four decades of research on bent functions. Des. Codes Cryptogr. **78**, 5–50 (2016).
7. Cusick, T. W., Dobbertin, H.: Some new three-valued crosscorrelation functions for binary m-sequences. IEEE Trans. Inform. Theory **42**, 1238–1240 (1996).
8. Dillon, J.: On the dimension of an APN code. Cryptogr. Commun. **3**, 275–279 (2011).
9. 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 (1987).
10. Ding, C.: Linear codes from some 2-designs. IEEE Trans. Inf. Theory **60**, 3265–3275 (2015).
11. Ding, C.: A construction of binary linear codes from Boolean functions. Disc. Math. **339**, 2288–2303 (2016).
12. Ding, C.: An infinite family of Steiner systems $S(2,4,2^m)$ from cyclic codes. J. Combinatorial Designs **26**, 127–144 (2018).
13. Ding, C.: Infinite families of t-designs from a type of five-weight codes. Des. Codes Cryptogr. **86**, 703–719 (2018).
14. Ding, C.: Designs from Linear Codes. World Scientific, Singapore (2018).
15. Ding, C., Li, C.: Infinite families of 2-designs and 3-designs from linear codes. Disc. Math. **340**, 2415–2431 (2017).
16. Ding, C., Munemasa, A., Tonchev, V.: Bent vectorial functions, codes and designs. arXiv:1808.08487v1 [math.CO].
17. Du, X., Wang, R., Fan, C.: Infinite families of 2-designs from a class of cyclic codes with two non-zeros. arXiv:1904.04242 [math.CO].
18. Du, X., Wang, R., Tang, C., Wang, Q.: Infinite families of 2-designs from two classes of binary cyclic codes with three nonzeros. arXiv:1903.08153 [math.CO].
19. Du, X., Wang, R., Tang, C., Wang, Q.: Infinite families of 2-designs from two classes of linear codes. arXiv:1903.07459 [math.CO].
20. Feng, K., Luo, J.: Value distributions of exponential sums from perfect nonlinear functions and their applications. IEEE Trans. Inf. Theory **53**, 3053–3041 (2007).
21. Gold, R.: Maximal recursive sequences with 3-valued recursive cross-correlation functions. IEEE Trans. Inf. Theory **14**, 154–156 (1967).
22. Huffman, W. C., Pless, V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).
23. 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).
24. Kantor, W. M.: Symplectic groups, symmetric designs, and line ovals. J. Algebra **33**, 43–58 (1975).
25. Kantor, W. M.: Exponential number of two-weight codes, difference sets and symmetric designs. Disc. Math. **46**, 95–98 (1983).
26. Kasami, T.: Weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Information and Control **18**, 369–394 (1971).
27. Kasami, T., Lin, S., Peterson, W. W.: Some results on cyclic codes which are invariant under the affine group and their applications. Information and Control **11**, 475–496 (1968).

28. MacWilliams, F. J., Sloane, N. J. A.: The Theory of Error-Correcting Codes. North Holland, Amsterdam (1977).
29. McQuire, G.: Quasi-symmetric designs and codes meeting the Grey-Rankin bound. J. Comb. Theory A **78**, 280–291 (1997).
30. Mesnager, S.: Bent Functions: Fundamentals and Results. Springer Verlag, Switzerland (2016).
31. Pott, A.: Almost perfect and planar functions. Des. Codes Cryptogr. **78**, 141–195 (2016).
32. Tonchev, V. D.: Quasi-symmetric designs, codes, quadrics, and hyperplane sections. Geometriae Dedicata **48**, 295–308 (1993).
33. Van Lint, J. H.: Introduction to Coding Theory, Third Edition. Springer Verlag, New York (1999).
34. Wolfmann, J.: Bent functions and coding theory. In: Difference Sets, Sequences and their Correlation Properties, A. Pott, P. V. Kumar, T. Helleseth and D. Jungnickel, eds., pp. 393–417. Amsterdam: Kluwer (1999).
35. Xiang, C., Ding, C., Mesnager, S.: Optimal codebooks from binary codes meeting the Levenshtein bound. IEEE Trans. Inf. Theory **61**, 6526–6535 (2015).
36. Yuan, J., Carlet, C., Ding, C: The weight distribution of a class of linear codes from perfect nonlinear functions. IEEE Trans. Inf. Theory **52**, 712–717 (2006).