Des. Codes Cryptogr. (2018) 86:703–719
https://doi.org/10.1007/s10623-017-0352-6

CrossMark

Infinite families of 3-designs from a type of five-weight code

Cunsheng Ding[1]

Received: 18 August 2016 / Accepted: 6 March 2017 / Published online: 15 March 2017

Abstract It has been known for a long time that t-designs can be employed to construct both linear and nonlinear codes and that the codewords of a fixed weight in a code may hold a t-design. While a lot of progress in the direction of constructing codes from t-designs has been made, only a small amount of work on the construction of t-designs from codes has been done. The objective of this paper is to construct infinite families of 2-designs and 3-designs from a type of binary linear codes with five weights. The total number of 2-designs and 3-designs obtained in this paper are exponential in any odd m and the block size of the designs varies in a huge range.

Keywords Cyclic code · Linear code · Weight distribution · t-design

Mathematics Subject Classification 94B05 · 94B15 · 05B05

1 Introduction

We start with a brief recall of t-designs. 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 paper, 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 paper, we consider only

Communicated by L. Teirlinck.

✉ Cunsheng Ding
cding@ust.hk

1 Department of Computer Science and Engineering, The Hong Kong University of Science and Technology, Clear Water Bay, Jiulong, Hong Kong, China

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 $S(t, k, v)$.

A necessary condition for the existence of a t-(v, k, λ) design is that

$$\binom{k-i}{t-i} \text{ divides } \lambda \binom{v-i}{t-i}, \tag{1}$$

for all integer i with $0 \leq i \leq t$.

The interplay between codes and t-designs goes in two directions. In one direction, the incidence matrix of any t-design generates a linear code over any finite field GF(q). A lot of progress in this direction has been made and documented in the literature (see, for examples, [1,5,19,20]). In the other direction, the codewords of a fixed Hamming weight in a linear or nonlinear code may hold a t-design. Some linear and nonlinear codes were employed to construct t-designs [1,10,12,14,16,18–20]. Binary and ternary Golay codes of certain parameters give 4-designs and 5-designs with fixed parameters. However, the largest t for which an infinite family of t-designs is derived directly from codes is $t = 3$. According to [1,13,19,20], not much progress on the construction of t-designs from codes has been made so far, while many other constructions of t-designs are documented in the literature [3,4,13,15,17]. The first motivation of this paper is to demonstrate that exponentially many infinite families of 3-designs could be constructed from linear codes. The second motivation is the important applications of t-designs in coding theory, cryptography, communications and statistics.

The objective of this paper is to construct infinite families of 2-designs and 3-designs from a type of binary linear codes with five weights. The obtained t-designs depend only on the weight distribution of the underlying binary codes. The total number of 2-designs and 3-designs presented in this paper are exponential in m, where $m \geq 5$ is an odd integer. In addition, the block size of the designs can vary in a huge range.

2 The classical construction of t-designs from codes

Let $\mathcal{C}$ be a $[v, \kappa, d]$ linear code over GF(q). Let $A_i := A_i(\mathcal{C})$, which denotes the number of codewords with Hamming weight i in $\mathcal{C}$, where $0 \leq i \leq v$. The sequence $(A_0, A_1, \ldots, A_v)$ is called the *weight distribution* of $\mathcal{C}$, and $\sum_{i=0}^{v} A_i z^i$ is referred to as the *weight enumerator* of $\mathcal{C}$. 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 $\mathcal{C}$, where the coordinates of a codeword are indexed by $(0, 1, 2, \ldots, v-1)$. Let $\mathcal{P} = \{0, 1, 2, \ldots, v-1\}$. The pair $(\mathcal{P}, \mathcal{B}_k)$ may be a t-(v, k, λ) design for some positive integer λ. The following theorems, developed by Assmus and Mattson, show that the pair $(\mathcal{P}, \mathcal{B}_k)$ defined by a linear code is a t-design under certain conditions.

Theorem 1 (Assmus–Mattson Theorem [2,9], p. 303) *Let $\mathcal{C}$ be a binary $[v, \kappa, d]$ code. Suppose $\mathcal{C}^{\perp}$ has minimum weight $d^{\perp}$. Suppose that $A_i = A_i(\mathcal{C})$ and $A_i^{\perp} = A_i(\mathcal{C}^{\perp})$, for $0 \leq i \leq v$, are the weight distributions of $\mathcal{C}$ and $\mathcal{C}^{\perp}$, respectively. Fix a positive integer t with $t < d$, and let s be the number of i with $A_i^{\perp} \neq 0$ for $0 < i \leq v - t$. Suppose that $s \leq d - t$. Then*

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

To construct t-designs via Theorem 1, we will need the following lemma in subsequent sections, which is a variant of the MacWilliam Identity [21, p. 41].

Theorem 2 *Let $\mathcal{C}$ be a $[v, \kappa, d]$ code over* GF(q) *with weight enumerator $A(z) = \sum_{i=0}^{v} A_i z^i$ and let $A^{\perp}(z)$ be the weight enumerator of $\mathcal{C}^{\perp}$. Then*

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

Later in this paper, we will need also the following theorem.

Theorem 3 *Let $\mathcal{C}$ be an $[n, k, d]$ binary linear code, and let $\mathcal{C}^{\perp}$ denote the dual of $\mathcal{C}$. Denote by $\overline{\mathcal{C}^{\perp}}$ the extended code of $\mathcal{C}^{\perp}$, and let $\overline{\mathcal{C}^{\perp}}^{\perp}$ denote the dual of $\overline{\mathcal{C}^{\perp}}$. Then we have the following.*

(1) *$\mathcal{C}^{\perp}$ has parameters $[n, n-k, d^{\perp}]$, where $d^{\perp}$ denotes the minimum distance of $\mathcal{C}^{\perp}$.*
(2) *$\overline{\mathcal{C}^{\perp}}$ has parameters $[n+1, n-k, \overline{d^{\perp}}]$, where $\overline{d^{\perp}}$ denotes the minimum distance of $\overline{\mathcal{C}^{\perp}}$, and is given by*

$$\overline{d^{\perp}} = \begin{cases} d^{\perp} & \text{if } d^{\perp} \text{ is even,} \\ d^{\perp}+1 & \text{if } d^{\perp} \text{ is odd.} \end{cases}$$

(3) *$\overline{\mathcal{C}^{\perp}}^{\perp}$ has parameters $[n+1, k+1, \overline{d^{\perp}}^{\perp}]$, where $\overline{d^{\perp}}^{\perp}$ denotes the minimum distance of $\overline{\mathcal{C}^{\perp}}^{\perp}$. Furthermore, $\overline{\mathcal{C}^{\perp}}^{\perp}$ has only even-weight codewords, and all the nonzero weights in $\overline{\mathcal{C}^{\perp}}^{\perp}$ are the following:*

$$w_1, w_2, \ldots, w_t; \; n+1-w_1, n+1-w_2, \ldots, n+1-w_t; \; n+1,$$

where $w_1, w_2, \ldots, w_t$ denote all the nonzero weights of $\mathcal{C}$.

Proof The conclusions of the first two parts are straightforward. We prove only the conclusions of the third part below.

Since $\overline{\mathcal{C}^{\perp}}$ has length $n+1$ and dimension $n-k$, the dimension of $\overline{\mathcal{C}^{\perp}}^{\perp}$ is $k+1$. By assumption, all codes under consideration are binary. By definition, $\overline{\mathcal{C}^{\perp}}$ has only even-weight codewords. Recall that $\overline{\mathcal{C}^{\perp}}$ is the extended code of $\mathcal{C}^{\perp}$. It is known that the generator matrix of $\overline{\mathcal{C}^{\perp}}^{\perp}$ is given by [9, p. 15]

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

where $\bar{\mathbf{1}} = (111\cdots1)$ is the all-one vector of length n, $\bar{\mathbf{0}} = (000\cdots0)^T$, which is a column vector of length n, and G is the generator matrix of $\mathcal{C}$. Notice again that $\overline{\mathcal{C}^{\perp}}^{\perp}$ is binary, the desired conclusions on the weights in $\overline{\mathcal{C}^{\perp}}^{\perp}$ follow from the relation between the two generator matrices of the two codes $\overline{\mathcal{C}^{\perp}}^{\perp}$ and $\mathcal{C}$. □

3 A type of binary linear codes with five-weights and related codes

In this section, we first introduce a type of binary linear codes $\mathcal{C}_m$ of length $n = 2^m - 1$, which has the weight distribution of Table 1, and then analyze their dual codes $\mathcal{C}_m^{\perp}$, the extended codes $\overline{\mathcal{C}_m^{\perp}}$, and the duals $\overline{\mathcal{C}_m^{\perp}}^{\perp}$. Such codes will be employed to construct t-designs in Sects. 4 and 5. Examples of such codes will be given in Sect. 6.

Table 1 The weight distribution of $\mathcal{C}_m$ for odd m

Weight w	No. of codewords A_w
0	1
$2^{m-1}-2^{(m+1)/2}$	$(2^m-1)\cdot 2^{(m-5)/2}\cdot(2^{(m-3)/2}+1)\cdot(2^{m-1}-1)/3$
$2^{m-1}-2^{(m-1)/2}$	$(2^m-1)\cdot 2^{(m-3)/2}\cdot(2^{(m-1)/2}+1)\cdot(5\cdot 2^{m-1}+4)/3$
2^{m-1}	$(2^m-1)\cdot(9\cdot 2^{2m-4}+3\cdot 2^{m-3}+1)$
$2^{m-1}+2^{(m-1)/2}$	$(2^m-1)\cdot 2^{(m-3)/2}\cdot(2^{(m-1)/2}-1)\cdot(5\cdot 2^{m-1}+4)/3$
$2^{m-1}+2^{(m+1)/2}$	$(2^m-1)\cdot 2^{(m-5)/2}\cdot(2^{(m-3)/2}-1)\cdot(2^{m-1}-1)/3$

Theorem 4 *Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the dual code $\mathcal{C}_m^{\perp}$ has parameters $[2^m-1,\ 2^m-1-3m,\ 7]$, and its weight distribution is given by*

$$2^{3m}A_k^{\perp} = \binom{2^m-1}{k} + aU_a(k) + bU_b(k) + cU_c(k) + dU_d(k) + eU_e(k),$$

where $0 \leq k \leq 2^m-1$,

$$\begin{aligned}
a &= \left(2^m-1\right)2^{(m-5)/2}\left(2^{(m-3)/2}+1\right)\left(2^{m-1}-1\right)/3,\\
b &= \left(2^m-1\right)2^{(m-3)/2}\left(2^{(m-1)/2}+1\right)\left(5\times 2^{m-1}+4\right)/3,\\
c &= \left(2^m-1\right)\left(9\times 2^{2m-4}+3\times 2^{m-3}+1\right),\\
d &= \left(2^m-1\right)2^{(m-3)/2}\left(2^{(m-1)/2}-1\right)\left(5\times 2^{m-1}+4\right)/3,\\
e &= \left(2^m-1\right)2^{(m-5)/2}\left(2^{(m-3)/2}-1\right)\left(2^{m-1}-1\right)/3,
\end{aligned}$$

and

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

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

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

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

$$U_e(k) = \sum_{\substack{0 \le i \le 2^{m-1}+2^{(m+1)/2} \\ 0 \le j \le 2^{m-1}-2^{(m+1)/2}-1 \\ i+j=k}} (-1)^i \binom{2^{m-1}+2^{(m+1)/2}}{i} \binom{2^{m-1}-2^{(m+1)/2}-1}{j}.$$

Proof By assumption, the weight enumerator of $\mathcal{C}_m$ is given by

$$A(z) = 1 + az^{2^{m-1}-2^{(m+1)/2}} + bz^{2^{m-1}-2^{(m-1)/2}} + cz^{2^{m-1}} + dz^{2^{m-1}+2^{(m-1)/2}} + ez^{2^{m-1}+2^{(m+1)/2}}.$$

It then follows from Theorem 2 that the weight enumerator of $\mathcal{C}_m^{\perp}$ is given by

$$2^{3m}A^{\perp}(z) = (1+z)^{2^m-1}\left[1 + a\left(\frac{1-z}{1+z}\right)^{2^{m-1}-2^{\frac{m+1}{2}}} + b\left(\frac{1-z}{1+z}\right)^{2^{m-1}-2^{\frac{m-1}{2}}}\right]$$
$$+(1+z)^{2^m-1}\left[c\left(\frac{1-z}{1+z}\right)^{2^{m-1}} + d\left(\frac{1-z}{1+z}\right)^{2^{m-1}+2^{\frac{m-1}{2}}} + e\left(\frac{1-z}{1+z}\right)^{2^{m-1}+2^{\frac{m+1}{2}}}\right].$$

Hence, we have

$$\begin{aligned}
2^{3m}A^{\perp}(z) = (1+z)^{2^m-1} & \\
& +a(1-z)^{2^{m-1}-2^{(m+1)/2}}(1+z)^{2^{m-1}+2^{(m+1)/2}-1} \\
& +b(1-z)^{2^{m-1}-2^{(m-1)/2}}(1+z)^{2^{m-1}+2^{(m-1)/2}-1} \\
& +c(1-z)^{2^{m-1}}(1+z)^{2^{m-1}-1} \\
& +d(1-z)^{2^{m-1}+2^{(m-1)/2}}(1+z)^{2^{m-1}-2^{(m-1)/2}-1} \\
& +e(1-z)^{2^{m-1}+2^{(m+1)/2}}(1+z)^{2^{m-1}-2^{(m+1)/2}-1}.
\end{aligned}$$

Obviously, we have

$$(1+z)^{2^m-1} = \sum_{k=0}^{2^m-1} \binom{2^m-1}{k} z^k.$$

It is easily seen that

$$(1-z)^{2^{m-1}-2^{(m+1)/2}}(1+z)^{2^{m-1}+2^{(m+1)/2}-1} = \sum_{k=0}^{2^m-1} U_a(k)z^k,$$

and

$$(1-z)^{2^{m-1}-2^{(m-1)/2}}(1+z)^{2^{m-1}+2^{(m-1)/2}-1} = \sum_{k=0}^{2^m-1} U_b(k)z^k.$$

Similarly,

$$(1-z)^{2^{m-1}+2^{(m-1)/2}}(1+z)^{2^{m-1}-2^{(m-1)/2}-1} = \sum_{k=0}^{2^m-1} U_d(k)z^k,$$

and

$$(1-z)^{2^{m-1}+2^{(m+1)/2}}(1+z)^{2^{m-1}-2^{(m+1)/2}-1} = \sum_{k=0}^{2^m-1} U_e(k)z^k.$$

Finally, we have

$$(1-z)^{2^{m-1}}(1+z)^{2^{m-1}-1} = \sum_{k=0}^{2^m-1} U_c(k)z^k.$$

Combining these formulas above yields the weight distribution formula for $A_k^{\perp}$.

The weight distribution in Table 1 tells us that the dimension of $\mathcal{C}_m$ is $3m$. Therefore, the dimension of $\mathcal{C}_m^{\perp}$ is equal to $2^m - 1 - 3m$. Finally, we prove that the minimum distance of $\mathcal{C}_m^{\perp}$ equals 7.

We now prove that $A_k^{\perp} = 0$ for all k with $1 \le k \le 6$. Let $x = 2^{(m-1)/2}$. With the weight distribution formula for $\mathcal{C}_m^{\perp}$ obtained before, we have

$$\begin{aligned}
\binom{2^m-1}{1} &= 2x^2 - 1,\\
aU_a(1) &= \frac{1}{3}x^7 + \frac{7}{12}x^6 - \frac{2}{3}x^5 - \frac{7}{8}x^4 + \frac{5}{12}x^3 + \frac{7}{24}x^2 - \frac{1}{12}x,\\
bU_b(1) &= \frac{10}{3}x^7 + \frac{5}{3}x^6 - \frac{2}{3}x^5 + \frac{1}{2}x^4 - \frac{11}{6}x^3 - \frac{2}{3}x^2 + \frac{2}{3}x,\\
cU_c(1) &= -\frac{9}{2}x^6 + \frac{3}{4}x^4 - \frac{5}{4}x^2 + 1,\\
dU_d(1) &= -\frac{10}{3}x^7 + \frac{5}{3}x^6 + \frac{2}{3}x^5 + \frac{1}{2}x^4 + \frac{11}{6}x^3 - \frac{2}{3}x^2 - \frac{2}{3}x,\\
eU_e(1) &= -\frac{1}{3}x^7 + \frac{7}{12}x^6 + \frac{2}{3}x^5 - \frac{7}{8}x^4 - \frac{5}{12}x^3 + \frac{7}{24}x^2 + \frac{1}{12}x.
\end{aligned}$$

Consequently,

$$2^{3m}A_1^{\perp} = \binom{2^m-1}{1} + aU_a(1) + bU_b(1) + cU_c(1) + dU_d(1) + eU_e(1) = 0.$$

Plugging $k = 2$ into the weight distribution formula above for $\mathcal{C}_m^{\perp}$, we get that

$$\begin{aligned}
\binom{2^m-1}{2} &= 2x^4 - 3x^2 + 1,\\
aU_a(2) &= \frac{7}{12}x^8 + \frac{5}{6}x^7 - \frac{35}{24}x^6 - \frac{13}{12}x^5 + \frac{7}{6}x^4 + \frac{1}{6}x^3 - \frac{7}{24}x^2 + \frac{1}{12}x,\\
bU_b(2) &= \frac{5}{3}x^8 - \frac{5}{3}x^7 - \frac{7}{6}x^6 + \frac{7}{6}x^5 - \frac{7}{6}x^4 + \frac{7}{6}x^3 + \frac{2}{3}x^2 - \frac{2}{3}x,\\
cU_c(2) &= -\frac{9}{2}x^8 + \frac{21}{4}x^6 - 2x^4 + \frac{9}{4}x^2 - 1,\\
dU_d(2) &= \frac{5}{3}x^8 + \frac{5}{3}x^7 - \frac{7}{6}x^6 - \frac{7}{6}x^5 - \frac{7}{6}x^4 - \frac{7}{6}x^3 + \frac{2}{3}x^2 + \frac{2}{3}x,\\
eU_e(2) &= \frac{7}{12}x^8 - \frac{5}{6}x^7 - \frac{35}{24}x^6 + \frac{13}{12}x^5 + \frac{7}{6}x^4 - \frac{1}{6}x^3 - \frac{7}{24}x^2 - \frac{1}{12}x.
\end{aligned}$$

As a result,

$$2^{3m}A_2^{\perp} = \binom{2^m-1}{2} + aU_a(2) + bU_b(2) + cU_c(2) + dU_d(2) + eU_e(2) = 0.$$

Putting $k = 3$ into the weight distribution formula above for $\mathcal{C}_m^{\perp}$, we obtain that

$$\binom{2^m-1}{3} = \frac{4}{3}x^6 - 4x^4 + \frac{11}{3}x^2 - 1,$$

$$aU_a(3) = \frac{5}{9}x^9 + \frac{19}{36}x^8 - \frac{14}{9}x^7 + \frac{1}{72}x^6 + \frac{43}{36}x^5 - \frac{17}{18}x^4 - \frac{1}{9}x^3 + \frac{29}{72}x^2 - \frac{1}{12}x,$$

$$bU_b(3) = -\frac{10}{9}x^9 - \frac{25}{9}x^8 + \frac{22}{9}x^7 + \frac{35}{18}x^6 - \frac{7}{18}x^5 + \frac{35}{18}x^4 - \frac{29}{18}x^3 - \frac{10}{9}x^2 + \frac{2}{3}x,$$

$$cU_c(3) = \frac{9}{2}x^8 - \frac{21}{4}x^6 + 2x^4 - \frac{9}{4}x^2 + 1,$$

$$dU_d(3) = \frac{10}{9}x^9 - \frac{25}{9}x^8 - \frac{22}{9}x^7 + \frac{35}{18}x^6 + \frac{7}{18}x^5 + \frac{35}{18}x^4 + \frac{29}{18}x^3 - \frac{10}{9}x^2 - \frac{2}{3}x,$$

$$eU_e(3) = -\frac{5}{9}x^9 + \frac{19}{36}x^8 + \frac{14}{9}x^7 + \frac{1}{72}x^6 - \frac{43}{36}x^5 - \frac{17}{18}x^4 + \frac{1}{9}x^3 + \frac{29}{72}x^2 + \frac{1}{12}x.$$

Hence,

$$2^{3m}A_3^{\perp} = \binom{2^m-1}{3} + aU_a(3) + bU_b(3) + cU_c(3) + dU_d(3) + eU_e(3) = 0.$$

Plugging $k = 4$ into the weight distribution formula above for $\mathcal{C}_m^{\perp}$, we get that

$$\binom{2^m-1}{4} = \frac{2}{3}x^8 - \frac{10}{3}x^6 + \frac{35}{6}x^4 - \frac{25}{6}x^2 + 1,$$

$$aU_a(4) = \frac{19}{72}x^{10} - \frac{1}{36}x^9 - \frac{25}{48}x^8 + \frac{113}{72}x^7 - \frac{35}{72}x^6 - \frac{77}{36}x^5 + \frac{55}{48}x^4 + \frac{37}{72}x^3 - \frac{29}{72}x^2 + \frac{1}{12}x,$$

$$bU_b(4) = -\frac{25}{18}x^{10} - \frac{5}{18}x^9 + \frac{15}{4}x^8 - \frac{53}{36}x^7 - \frac{35}{36}x^6 + \frac{49}{36}x^5 - \frac{5}{2}x^4 + \frac{19}{18}x^3 + \frac{10}{9}x^2 - \frac{2}{3}x,$$

$$cU_c(4) = \frac{9}{4}x^{10} - \frac{57}{8}x^8 + \frac{25}{4}x^6 - \frac{25}{8}x^4 + \frac{11}{4}x^2 - 1,$$

$$dU_d(4) = -\frac{25}{18}x^{10} + \frac{5}{18}x^9 + \frac{15}{4}x^8 + \frac{53}{36}x^7 - \frac{35}{36}x^6 - \frac{49}{36}x^5 - \frac{5}{2}x^4 - \frac{19}{18}x^3 + \frac{10}{9}x^2 + \frac{2}{3}x,$$

$$eU_e(4) = \frac{19}{72}x^{10} + \frac{1}{36}x^9 - \frac{25}{48}x^8 - \frac{113}{72}x^7 - \frac{35}{72}x^6 + \frac{77}{36}x^5 + \frac{55}{48}x^4 - \frac{37}{72}x^3 - \frac{29}{72}x^2 - \frac{1}{12}x.$$

Consequently,

$$2^{3m}A_4^{\perp} = \binom{2^m-1}{4} + aU_a(4) + bU_b(4) + cU_c(4) + dU_d(4) + eU_e(4) = 0.$$

Putting $k = 5$ into the weight distribution formula above for $\mathcal{C}_m^{\perp}$, we obtain that

$$\binom{2^m-1}{5} = \frac{4}{15}x^{10} - 2x^8 + \frac{17}{3}x^6 - \frac{15}{2}x^4 + \frac{137}{30}x^2 - 1,$$

$$\begin{aligned}
aU_a(5) &= -\frac{1}{90}x^{11} - \frac{103}{360}x^{10} + \frac{59}{90}x^9 + \frac{1279}{720}x^8 - \frac{97}{40}x^7 - \frac{49}{40}x^6 + \frac{211}{90}x^5 \\
&\quad -\frac{529}{720}x^4 - \frac{173}{360}x^3 + \frac{169}{360}x^2 - \frac{1}{12}x, \\
bU_b(5) &= -\frac{1}{9}x^{11} + \frac{23}{18}x^{10} - \frac{14}{45}x^9 - \frac{781}{180}x^8 + \frac{121}{60}x^7 + \frac{91}{60}x^6 - \frac{169}{180}x^5 \\
&\quad +\frac{263}{90}x^4 - \frac{119}{90}x^3 - \frac{62}{45}x^2 + \frac{2}{3}x, \\
cU_c(5) &= -\frac{9}{4}x^{10} + \frac{57}{8}x^8 - \frac{25}{4}x^6 + \frac{25}{8}x^4 - \frac{11}{4}x^2 + 1, \\
dU_d(5) &= \frac{1}{9}x^{11} + \frac{23}{18}x^{10} + \frac{14}{45}x^9 - \frac{781}{180}x^8 - \frac{121}{60}x^7 + \frac{91}{60}x^6 + \frac{169}{180}x^5 \\
&\quad +\frac{263}{90}x^4 + \frac{119}{90}x^3 - \frac{62}{45}x^2 - \frac{2}{3}x, \\
eU_e(5) &= \frac{1}{90}x^{11} - \frac{103}{360}x^{10} - \frac{59}{90}x^9 + \frac{1279}{720}x^8 + \frac{97}{40}x^7 - \frac{49}{40}x^6 - \frac{211}{90}x^5 \\
&\quad -\frac{529}{720}x^4 + \frac{173}{360}x^3 + \frac{169}{360}x^2 + \frac{1}{12}x.
\end{aligned}$$

Consequently,

$$2^{3m}A_5^{\perp} = \binom{2^m-1}{5} + aU_a(5) + bU_b(5) + cU_c(5) + dU_d(5) + eU_e(5) = 0.$$

Plugging $k = 6$ into the weight distribution formula above for $\mathcal{C}_m^{\perp}$, we arrive at that

$$\begin{aligned}
\binom{2^m-1}{6} &= \frac{4}{45}x^{12} - \frac{14}{15}x^{10} + \frac{35}{9}x^8 - \frac{49}{6}x^6 + \frac{406}{45}x^4 - \frac{49}{10}x^2 + 1, \\
aU_a(6) &= -\frac{103}{1080}x^{12} - \frac{97}{540}x^{11} + \frac{1897}{2160}x^{10} + \frac{571}{1080}x^9 - \frac{1573}{720}x^8 + \frac{193}{120}x^7 \\
&\quad +\frac{2117}{2160}x^6 - \frac{3061}{1080}x^5 + \frac{385}{432}x^4 + \frac{857}{1080}x^3 - \frac{169}{360}x^2 + \frac{1}{12}x, \\
bU_b(6) &= \frac{23}{54}x^{12} + \frac{29}{54}x^{11} - \frac{1471}{540}x^{10} - \frac{613}{540}x^9 + \frac{218}{45}x^8 - \frac{68}{45}x^7 \\
&\quad -\frac{293}{540}x^6 + \frac{1033}{540}x^5 - \frac{913}{270}x^4 + \frac{233}{270}x^3 + \frac{62}{45}x^2 - \frac{2}{3}x, \\
cU_c(6) &= -\frac{3}{4}x^{12} + \frac{37}{8}x^{10} - \frac{221}{24}x^8 + \frac{175}{24}x^6 - \frac{97}{24}x^4 + \frac{37}{12}x^2 - 1, \\
dU_d(6) &= \frac{23}{54}x^{12} - \frac{29}{54}x^{11} - \frac{1471}{540}x^{10} + \frac{613}{540}x^9 + \frac{218}{45}x^8 + \frac{68}{45}x^7 \\
&\quad -\frac{293}{540}x^6 - \frac{1033}{540}x^5 - \frac{913}{270}x^4 - \frac{233}{270}x^3 + \frac{62}{45}x^2 + \frac{2}{3}x, \\
eU_e(6) &= -\frac{103}{1080}x^{12} + \frac{97}{540}x^{11} + \frac{1897}{2160}x^{10} - \frac{571}{1080}x^9 - \frac{1573}{720}x^8 - \frac{193}{120}x^7 \\
&\quad +\frac{2117}{2160}x^6 + \frac{3061}{1080}x^5 + \frac{385}{432}x^4 - \frac{857}{1080}x^3 - \frac{169}{360}x^2 - \frac{1}{12}x.
\end{aligned}$$

As a result,

$$2^{3m}A_6^{\perp} = \binom{2^m-1}{6} + aU_a(6) + bU_b(6) + cU_c(6) + dU_d(6) + eU_e(6) = 0.$$

Plugging $k = 7$ into the weight distribution formula above for $\mathcal{C}_m^{\perp}$, we obtain

$$\binom{2^m-1}{7} = \frac{8}{315}x^{14} - \frac{16}{45}x^{12} + \frac{92}{45}x^{10} - \frac{56}{9}x^{8} + \frac{967}{90}x^{6} - \frac{469}{45}x^{4} + \frac{363}{70}x^{2} - 1,$$

and

$$\begin{aligned} aU_a(7) &= -\frac{97}{1890}x^{13} - \frac{11}{1512}x^{12} + \frac{125}{378}x^{11} - \frac{8711}{15,120}x^{10} - \frac{523}{7560}x^{9} + \frac{15,643}{5040}x^{8} \\ &\quad - \frac{18,281}{7560}x^{7} - \frac{39,307}{15,120}x^{6} + \frac{23,141}{7560}x^{5} - \frac{6619}{15,120}x^{4} - \frac{5818}{7560}x^{3} + \frac{1303}{2520}x^{2} - \frac{1}{12}x, \\ bU_b(7) &= \frac{29}{189}x^{13} - \frac{103}{378}x^{12} - \frac{814}{945}x^{11} + \frac{9071}{3780}x^{10} + \frac{2659}{3780}x^{9} - \frac{554}{105}x^{8} + \frac{3889}{1890}x^{7} \\ &\quad + \frac{4117}{3780}x^{6} - \frac{6299}{3780}x^{5} + \frac{6857}{1890}x^{4} - \frac{1991}{1890}x^{3} - \frac{494}{315}x^{2} + \frac{2}{3}x, \\ cU_c(7) &= \frac{3}{4}x^{12} - \frac{37}{8}x^{10} + \frac{221}{24}x^{8} - \frac{175}{24}x^{6} + \frac{97}{24}x^{4} - \frac{37}{12}x^{2} + 1, \\ dU_d(7) &= -\frac{29}{189}x^{13} - \frac{103}{378}x^{12} + \frac{814}{945}x^{11} + \frac{9071}{3780}x^{10} - \frac{2659}{3780}x^{9} - \frac{554}{105}x^{8} - \frac{3889}{1890}x^{7} \\ &\quad + \frac{4117}{3780}x^{6} + \frac{6299}{3780}x^{5} + \frac{6857}{1890}x^{4} + \frac{1991}{1890}x^{3} - \frac{494}{315}x^{2} - \frac{2}{3}x, \\ eU_e(7) &= \frac{97}{1890}x^{13} - \frac{11}{1512}x^{12} - \frac{125}{378}x^{11} - \frac{8711}{15,120}x^{10} + \frac{523}{7560}x^{9} + \frac{15,643}{5040}x^{8} + \frac{18,281}{7560}x^{7} \\ &\quad - \frac{39,307}{15,120}x^{6} - \frac{23,141}{7560}x^{5} - \frac{6619}{15,120}x^{4} + \frac{5819}{7560}x^{3} + \frac{1303}{2520}x^{2} + \frac{1}{12}x. \end{aligned}$$

It then follows that

$$\begin{aligned} A_7^{\perp} &= 2^{-3m}\left(\binom{2^m-1}{7} + aU_a(7) + bU_b(7) + cU_c(7) + dU_d(7) + eU_e(7)\right) \\ &= \frac{(x^2-1)(2x^2-1)(x^4-5x^2+34)}{630}. \end{aligned}$$

Notice that $x^4 - 5x^2 + 34 = (x^2 - 5/2)^2 + 34 - 25/4 > 0$. We have $A_7^{\perp} > 0$ for all odd $m \geq 5$. This proves the desired conclusion on the minimum distance of $\mathcal{C}_m^{\perp}$. □

Theorem 5 *Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. The code $\overline{\mathcal{C}_m^{\perp}}^{\perp}$ has parameters*

$$\left[2^m,\ 3m+1,\ 2^{m-1} - 2^{(m+1)/2}\right],$$

and its weight enumerator is given by

$$\begin{aligned} \overline{A^{\perp}}^{\perp}(z) &= 1 + uz^{2^{m-1}-2^{\frac{m+1}{2}}} + vz^{2^{m-1}-2^{\frac{m-1}{2}}} \\ &\quad + wz^{2^{m-1}} + vz^{2^{m-1}+2^{\frac{m-1}{2}}} + uz^{2^{m-1}+2^{\frac{m+1}{2}}} + z^{2^m}, \end{aligned} \tag{2}$$

where

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

$$w = 2\left(2^m - 1\right)\left(9 \times 2^{2m-4} + 3 \times 2^{m-3} + 1\right).$$

Proof It follows from Theorem 3 that the code has all the weights given in (2). It remains to determine the frequencies of these weights. The weight distribution of the code $\mathcal{C}_m$ given in Table 1 and the generator matrix of the code $\overline{\mathcal{C}_m^\perp}^\perp$ documented in the proof of Theorem 3 show that

$$\overline{A^\perp}^\perp_{2^{m-1}} = 2c = w,$$

where c was defined in Theorem 4.

We now determine u and v. Recall that $\mathcal{C}_m^\perp$ has minimum distance 7. It then follows from Theorem 3 that $\overline{\mathcal{C}_m^\perp}$ has minimum distance 8. The first and third Pless power moments say that

$$\begin{cases} \sum_{i=0}^{2^m} \overline{A^\perp}^\perp_i = 2^{3m+1}, \\ \sum_{i=0}^{2^m} i^2 \overline{A^\perp}^\perp_i = 2^{3m-1} 2^m (2^m + 1). \end{cases}$$

These two equations become

$$\begin{cases} 1 + u + v + c = 2^{3m}, \\ (2^{2m-2} + 2^{m+1})u + (2^{2m-2} + 2^{m-1})v + 2^{2m-2}c + 2^{2m-1} = 2^{4m-2}(2^m + 1). \end{cases}$$

Solving this system of equations proves the desired conclusion on the weight enumerator of this code. □

Finally, we settle the weight distribution of the code $\overline{\mathcal{C}_m^\perp}$.

Theorem 6 *Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. The code $\overline{\mathcal{C}_m^\perp}$ has parameters $[2^m,\ 2^m - 1 - 3m,\ 8]$, and its weight distribution is given by*

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

where w, u, v are defined in Theorem 5, and

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

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

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

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

Proof By definition,

$$\dim\left(\overline{\mathcal{C}_m^\perp}\right) = \dim\left(\mathcal{C}_m^\perp\right) = 2^m - 1 - 3m.$$

It has been showed in the proof of Theorem 4 that the minimum distance of $\overline{\mathcal{C}_m^\perp}$ is equal to 8. We now prove the conclusion on the weight distribution of this code.

By Theorems 2 and 5, the weight enumerator of $\overline{\mathcal{C}_m^\perp}$ is given by

$$\begin{aligned} 2^{3m+1}\overline{A^\perp}(z) &= (1+z)^{2^m}\left[1+\left(\frac{1-z}{1+z}\right)^{2^m} + w\left(\frac{1-z}{1+z}\right)^{2^{m-1}}\right] \\ &\quad +(1+z)^{2^m}\left[u\left(\frac{1-z}{1+z}\right)^{2^{m-1}-2^{\frac{m+1}{2}}} + v\left(\frac{1-z}{1+z}\right)^{2^{m-1}-2^{\frac{m-1}{2}}}\right] \\ &\quad +(1+z)^{2^m}\left[v\left(\frac{1-z}{1+z}\right)^{2^{m-1}+2^{\frac{m-1}{2}}} + u\left(\frac{1-z}{1+z}\right)^{2^{m-1}+2^{\frac{m+1}{2}}}\right]. \end{aligned} \tag{4}$$

Consequently, we have

$$\begin{aligned} 2^{3m+1}\overline{A^\perp}(z) &= (1+z)^{2^m} + (1-z)^{2^m} + w(1-z^2)^{2^{m-1}} \\ &\quad +u(1-z)^{2^{m-1}-2^{(m+1)/2}}(1+z)^{2^{m-1}+2^{(m+1)/2}} \\ &\quad +v(1-z)^{2^{m-1}-2^{(m-1)/2}}(1+z)^{2^{m-1}+2^{(m-1)/2}} \\ &\quad +v(1-z)^{2^{m-1}+2^{(m-1)/2}}(1+z)^{2^{m-1}-2^{(m-1)/2}} \\ &\quad +u(1-z)^{2^{m-1}+2^{(m+1)/2}}(1+z)^{2^{m-1}-2^{(m+1)/2}}. \end{aligned} \tag{5}$$

We now treat the terms in (5) one by one. We first have

$$(1+z)^{2^m} + (1-z)^{2^m} = \sum_{k=0}^{2^m}\left(1+(-1)^k\right)\binom{2^m}{k}. \tag{6}$$

One can easily see that

$$\left(1-z^2\right)^{2^{m-1}} = \sum_{i=0}^{2^{m-1}}(-1)^i\binom{2^{m-1}}{i}z^{2i} = \sum_{k=0}^{2^m}\frac{1+(-1)^k}{2}(-1)^{\lfloor k/2\rfloor}\binom{2^{m-1}}{\lfloor k/2\rfloor}z^k. \tag{7}$$

Notice that

$$(1-z)^{2^{m-1}-2^{(m+1)/2}} = \sum_{i=0}^{2^{m-1}-2^{(m+1)/2}}\binom{2^{m-1}-2^{(m+1)/2}}{i}(-1)^i z^i,$$

and

$$(1+z)^{2^{m-1}+2^{(m+1)/2}} = \sum_{i=0}^{2^{m-1}+2^{(m+1)/2}}\binom{2^{m-1}+2^{(m+1)/2}}{i}z^i.$$

We have then

$$(1-z)^{2^{m-1}-2^{(m+1)/2}}(1+z)^{2^{m-1}+2^{(m+1)/2}} = \sum_{k=0}^{2^m}E_1(k)z^k. \tag{8}$$

Similarly, we have

$$(1-z)^{2^{m-1}-2^{(m-1)/2}}(1+z)^{2^{m-1}+2^{(m-1)/2}} = \sum_{k=0}^{2^m}E_2(k)z^k, \tag{9}$$

$$(1-z)^{2^{m-1}+2^{(m-1)/2}}(1+z)^{2^{m-1}-2^{(m-1)/2}} = \sum_{k=0}^{2^m} E_3(k)z^k, \quad (10)$$

$$(1-z)^{2^{m-1}+2^{(m+1)/2}}(1+z)^{2^{m-1}-2^{(m+1)/2}} = \sum_{k=0}^{2^m} E_4(k)z^k. \quad (11)$$

Plugging (6)–(11) into (5) proves the desired conclusion. □

4 Infinite families of 2-designs from $\mathcal{C}_m^{\perp}$ and $\mathcal{C}_m$

Theorem 7 *Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Let $\mathcal{P} = \{0, 1, 2, \ldots, 2^m - 2\}$, and let $\mathcal{B}$ be the set of the supports of the codewords of $\mathcal{C}_m$ with weight k, where $A_k \neq 0$. Then $(\mathcal{P}, \mathcal{B})$ is a 2-$(2^m - 1, k, \lambda)$ design, where*

$$\lambda = \frac{k(k-1)A_k}{(2^m-1)(2^m-2)},$$

where A_k is given in Table 1.

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

$$\lambda = \frac{k(k-1)A_k^{\perp}}{(2^m-1)(2^m-2)},$$

where $A_k^{\perp}$ is given in Theorem 4.

Proof The weight distribution of $\mathcal{C}_m^{\perp}$ is given in Theorem 4 and that of $\mathcal{C}_m$ is given in Table 1. By Theorem 4, the minimum distance $d^{\perp}$ of $\mathcal{C}_m^{\perp}$ is equal to 7. Put $t = 2$. The number of i with $A_i \neq 0$ and $1 \leq i \leq 2^m - 1 - t$ is $s = 5$. Hence, $s = d^{\perp} - t$. The desired conclusions then follow from Theorem 1 and the fact that two binary vectors have the same support if and only if they are equal. □

Example 1 Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the BCH code $\mathcal{C}_m$ holds five 2-designs with the following parameters:

- $(v, k, \lambda) = \left(2^m - 1,\ 2^{m-1} - 2^{\frac{m+1}{2}},\ \frac{2^{\frac{m-5}{2}}\left(2^{\frac{m-3}{2}}+1\right)\left(2^{m-1}-2^{\frac{m+1}{2}}\right)\left(2^{m-1}-2^{\frac{m+1}{2}}-1\right)}{6}\right).$
- $(v, k, \lambda) = \left(2^m - 1,\ 2^{m-1} - 2^{\frac{m-1}{2}},\ \frac{2^{m-2}\left(2^{m-1}-2^{\frac{m-1}{2}}-1\right)(5\times 2^{m-1}+4)}{6}\right).$
- $(v, k, \lambda) = \left(2^m - 1,\ 2^{m-1},\ 2^{m-2}\left(9 \times 2^{2m-4} + 3 \times 2^{m-3} + 1\right)\right).$
- $(v, k, \lambda) = \left(2^m - 1,\ 2^{m-1} + 2^{\frac{m-1}{2}},\ \frac{2^{m-2}\left(2^{m-1}+2^{\frac{m-1}{2}}-1\right)(5\times 2^{m-1}+4)}{6}\right).$
- $(v, k, \lambda) = \left(2^m - 1,\ 2^{m-1} + 2^{\frac{m+1}{2}},\ \frac{2^{\frac{m-5}{2}}\left(2^{\frac{m-3}{2}}-1\right)\left(2^{m-1}+2^{\frac{m+1}{2}}\right)\left(2^{m-1}+2^{\frac{m+1}{2}}-1\right)}{6}\right).$

Example 2 Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the supports of all codewords of weight 7 in $\mathcal{C}_m^\perp$ give a 2-$(2^m - 1, 7, \lambda)$ design, where

$$\lambda = \frac{2^{2(m-1)} - 5 \times 2^{m-1} + 34}{30}.$$

Proof By Theorem 4, we have

$$A_7^\perp = \frac{(2^{m-1} - 1)(2^m - 1)(2^{2(m-1)} - 5 \times 2^{m-1} + 34)}{630}.$$

The desired conclusion on λ follows from Theorem 7. □

Example 3 Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the supports of all codewords of weight 8 in $\mathcal{C}_m^\perp$ give a 2-$(2^m - 1, 8, \lambda)$ design, where

$$\lambda = \frac{(2^{m-1} - 4)(2^{2(m-1)} - 5 \times 2^{m-1} + 34)}{90}.$$

Proof By Theorem 4, we have

$$A_8^\perp = \frac{(2^{m-1} - 1)(2^{m-1} - 4)(2^m - 1)(2^{2(m-1)} - 5 \times 2^{m-1} + 34)}{2520}.$$

The desired conclusion on λ follows from Theorem 7. □

Example 4 Let $m \geq 7$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the supports of all codewords of weight 9 in $\mathcal{C}_m^\perp$ give a 2-$(2^m - 1, 9, \lambda)$ design, where

$$\lambda = \frac{(2^{m-1} - 4)(2^{m-1} - 16)(2^{2(m-1)} - 2^{m-1} + 28)}{315}.$$

Proof By Theorem 4, we have

$$A_9^\perp = \frac{(2^{m-1} - 1)(2^{m-1} - 4)(2^{m-1} - 16)(2^m - 1)(2^{2(m-1)} - 2^{m-1} + 28)}{11{,}340}.$$

The desired conclusion on λ follows from Theorem 7. □

5 Infinite families of 3-designs from $\overline{\mathcal{C}_m^\perp}$ and $\overline{\mathcal{C}_m^\perp}^\perp$

Theorem 8 *Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Let $\mathcal{P} = \{0, 1, 2, \ldots, 2^m - 1\}$, and let $\overline{\mathcal{B}^\perp}^\perp$ be the set of the supports of the codewords of $\overline{\mathcal{C}_m^\perp}^\perp$ with weight k, where $\overline{A^\perp}_k^\perp \neq 0$. Then $(\mathcal{P}, \overline{\mathcal{B}^\perp}^\perp)$ is a 3-$(2^m, k, \lambda)$ design, where*

$$\lambda = \frac{\overline{A^\perp}_k^\perp \binom{k}{3}}{\binom{2^m}{3}},$$

where $\overline{A^\perp}_k^\perp$ is given in Theorem 5.

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

$$\lambda = \frac{\overline{A^{\perp}}_k \binom{k}{3}}{\binom{2^m}{3}},$$

where $\overline{A^{\perp}}_k$ is given in Theorem 6.

Proof The weight distributions of $\overline{\mathcal{C}_m^{\perp}}^{\perp}$ and $\overline{\mathcal{C}_m^{\perp}}$ are described in Theorems 5 and 6. Notice that the minimum distance $\overline{d^{\perp}}$ of $\overline{\mathcal{C}_m^{\perp}}^{\perp}$ is equal to 8. Put $t = 3$. The number of i with $\overline{A^{\perp}}_i \neq 0$ and $1 \leq i \leq 2^m - t$ is $s = 5$. Hence, $s = \overline{d^{\perp}} - t$. Clearly, two binary vectors have the same support if and only if they are equal. The desired conclusions then follow from Theorem 1. □

Example 5 Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then $\overline{\mathcal{C}_m^{\perp}}^{\perp}$ holds five 3-designs with the following parameters:

- $(v, k, \lambda) = \left(2^m,\ 2^{m-1} - 2^{\frac{m+1}{2}},\ \frac{\left(2^{m-1}-2^{\frac{m+1}{2}}\right)\left(2^{m-1}-2^{\frac{m+1}{2}}-1\right)\left(2^{m-1}-2^{\frac{m+1}{2}}-2\right)}{48}\right).$
- $(v, k, \lambda) = \left(2^m,\ 2^{m-1} - 2^{\frac{m-1}{2}},\ \frac{2^{\frac{m-1}{2}}\left(2^{m-1}-2^{\frac{m-1}{2}}-1\right)\left(2^{\frac{m-1}{2}}-2\right)(5\times 2^{m-3}+1)}{3}\right).$
- $(v, k, \lambda) = \left(2^m,\ 2^{m-1},\ \left(2^{m-2}-1\right)\left(9 \times 2^{2m-4} + 3 \times 2^{m-3} + 1\right)\right).$
- $(v, k, \lambda) = \left(2^m,\ 2^{m-1} + 2^{\frac{m-1}{2}},\ \frac{2^{\frac{m-1}{2}}\left(2^{m-1}+2^{\frac{m-1}{2}}-1\right)\left(2^{\frac{m-1}{2}}+2\right)(5\times 2^{m-3}+1)}{3}\right).$
- $(v, k, \lambda) = \left(2^m,\ 2^{m-1} + 2^{\frac{m+1}{2}},\ \frac{\left(2^{m-1}+2^{\frac{m+1}{2}}\right)\left(2^{m-1}+2^{\frac{m+1}{2}}-1\right)\left(2^{m-1}+2^{\frac{m+1}{2}}-2\right)}{48}\right).$

Example 6 Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the supports of all codewords of weight 8 in $\overline{\mathcal{C}_m^{\perp}}$ give a 3-$(2^m, 8, \lambda)$ design, where

$$\lambda = \frac{2^{2(m-1)} - 5 \times 2^{m-1} + 34}{30}.$$

Proof By Theorem 6, we have

$$\overline{A^{\perp}}_8 = \frac{2^m(2^{m-1}-1)(2^m-1)(2^{2(m-1)} - 5 \times 2^{m-1} + 34)}{315}.$$

The desired value of λ follows from Theorem 8. □

Example 7 Let $m \geq 7$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the supports of all codewords of weight 10 in $\overline{\mathcal{C}_m^{\perp}}$ give a 3-$(2^m, 10, \lambda)$ design, where

$$\lambda = \frac{(2^{m-1}-4)(2^{m-1}-16)(2^{2(m-1)} - 2^{m-1} + 28)}{315}.$$

Proof By Theorem 6, we have

$$\overline{A^{\perp}}_{10} = \frac{2^{m-1}(2^{m-1}-1)(2^m-1)(2^{m-1}-4)(2^{m-1}-16)(2^{2(m-1)}-2^{m-1}+28)}{4\times 14{,}175}.$$

The desired value of λ follows from Theorem 8. □

Example 8 Let $m \geq 5$ be an odd integer and let $\mathcal{C}_m$ be a binary code with the weight distribution of Table 1. Then the supports of all codewords of weight 12 in $\overline{\mathcal{C}_m^{\perp}}$ give a 3-$(2^m,\ 12,\ \lambda)$ design, where

$$\lambda = \frac{(2^{h-2}-1)(2\times 2^{5h} - 55\times 2^{4h} + 647\times 2^{3h} - 2727\times 2^{2h} + 11{,}541\times 2^h - 47{,}208)}{2835},$$

and $h = m-1$.

Proof By Theorem 6, we have

$$\overline{A^{\perp}}_{12} = \frac{\epsilon^2(\epsilon^2-1)(\epsilon^2-4)(2\epsilon^2-1)(2\epsilon^{10}-55\epsilon^8+647\epsilon^6-2727\epsilon^4+11{,}541\epsilon^2-47{,}208)}{8\times 467{,}775},$$

where $\epsilon = 2^{(m-1)/2}$. The desired value of λ follows from Theorem 8. □

6 Two families of binary cyclic codes with the weight distribution of Table 1

To prove the existence of the 2-designs in Sect. 4 and the 3-designs in Sect. 5, we present two families of binary codes of length $2^m - 1$ with the weight distribution of Table 1.

Let $n = q^m - 1$, where m is a positive integer. Let α be a generator of $\mathrm{GF}(q^m)^*$. For any i with $0 \leq i \leq n-1$, let $\mathbb{M}_i(x)$ denote the minimal polynomial of β^i over $\mathrm{GF}(q)$. For any $2 \leq \delta \leq n$, define

$$g_{(q,n,\delta,b)}(x) = \mathrm{lcm}\left(\mathbb{M}_b(x),\ \mathbb{M}_{b+1}(x), \ldots, \mathbb{M}_{b+\delta-2}(x)\right), \tag{12}$$

where b is an integer, lcm denotes the least common multiple of these minimal polynomials, and the addition in the subscript $b+i$ of $\mathbb{M}_{b+i}(x)$ always means the integer addition modulo n. Let $\mathcal{C}_{(q,n,\delta,b)}$ denote the cyclic code of length n with generator polynomial $g_{(q,n,\delta,b)}(x)$. $\mathcal{C}_{(q,n,\delta,b)}$ is called a *primitive BCH code* with *designed distance* δ. When $b = 1$, the set $\mathcal{C}_{(q,n,\delta,b)}$ is called a *narrow-sense primitive BCH code*.

Although primitive BCH codes are not asymptotically good, they are among the best linear codes when the length of the codes is not very large [5, Appendix A]. So far, we have very limited knowledge of BCH codes, as the dimension and minimum distance of BCH codes are in general open, in spite of some recent progress [6,7]. However, in a few cases the weight distribution of a BCH code can be settled. The following theorem introduces such a case.

Theorem 9 *Let $m \geq 5$ be an odd integer and let $\delta = 2^{m-1} - 1 - 2^{(m+1)/2}$. Then the BCH code $\mathcal{C}_{(2,2^m-1,\delta,0)}$ has length $n = 2^m - 1$, dimension $3m$, and the weight distribution in Table 1.*

Proof A proof can be found in [8]. □

It is known that the dual of a BCH code may not be a BCH code. The following theorem describes a family of cyclic codes having the weight distribution of Table 1, which may not be BCH codes.

Theorem 10 *Let $m \geq 5$ be an odd integer. Let $\mathcal{C}_m$ be the dual of the narrow-sense primitive BCH code $\mathcal{C}_{(2,2^m-1,7,1)}$. Then $\mathcal{C}_m$ has the weight distribution of Table 1.*

Proof A proof can be found in [11]. □

7 Summary and concluding remarks

In this paper, with any binary linear code of length 2^m-1 and the weight distribution of Table 1, exponentially many infinite families of 2-designs and 3-designs with various block sizes were constructed with only one strike. These designs depend only on the weight distribution of the underlying linear code $\mathcal{C}_m$, and do not depend on the specific construction of the linear code $\mathcal{C}_m$. In other words, one can tell you that your code and its associated codes (the dual code, the extended code of the dual code) hold exponentially many 2-designs and 3-designs if you only tell him/her that you have a binary linear code with the weight distribution of Table 1 without giving further information of your linear code. This fact makes Theorems 7 and 8 different from theorems on t-designs from codes documented in the literature, which need the description of the specific construction of the underlying code. In summary, Theorems 7 and 8 are more specific than the original Assmus–Mattson Theorem, as they work only for a type of linear codes with five weights. They are more general than other theorems on t-designs, as most theorems on t-designs in the literature apply only to a specific linear code.

Given only the weight distribution of a linear code, it might be impossible to determine the automorphism group of the linear code. Thus, Theorems 7 and 8 may not be proved with the automorphism group approach. Therefore, the proofs of 7 and 8 given in the paper may be the only choice. For the same reason, the proofs of Theorems 4 and 6 presented in this paper may not have a choice, though they are complicated and tedious.

The constructions of the exponentially many infinite families of 3-designs presented in this paper demonstrate that the coding theory approach to constructing t-designs may be promising, and may stimulate further investigations in this direction. However, it is open if the codewords of a fixed weight in a family of linear codes can hold an infinite family of t-designs for some $t \geq 4$.

Acknowledgements C. Ding's research was supported by the Hong Kong Research Grants Council, Proj. No. 16300415.

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.: Coding and combinatorics. SIAM Rev. **16**, 349–388 (1974).
3. Beth T., Jungnickel D., Lenz H.: Design Theory. Cambridge University Press, Cambridge (1999).
4. Colbourn C.J., Mathon R.: Steiner systems. In: Colbourn C.J., Dinitz J. (eds.) Handbook of Combinatorial Designs, pp. 102–110. CRC Press, Boca Raton (2007).
5. Ding C.: Codes from Difference Sets. World Scientific, Singapore (2015).
6. Ding C.: Parameters of several classes of BCH codes. IEEE Trans. Inf. Theory **61**, 5322–5330 (2015).
7. Ding C., Du X., Zhou Z.: The Bose and minimum distance of a class of BCH codes. IEEE Trans. Inf. Theory **61**, 2351–2356 (2015).
8. Ding C., Fan C., Zhou Z.: The dimension and minimum distance of two classes of primitive BCH codes. Finite Fields Appl. **45**, 237–263 (2017).
9. Huffman W.C., Pless V.: Fundamentals of Error-Correcting Codes. Cambridge University Press, Cambridge (2003).

10. Jungnickel D., Tonchev V.D.: Exponential number of quasi-symmetric SDP designs and codes meeting the Grey–Rankin bound. Des. Codes Cryptogr. **1**, 247–253 (1991).
11. Kasami T.: Chapter 20, weight distributions of Bose–Chaudhuri–Hocquenghem codes. In: Bose R.C., Dowlings T.A. (eds.) Combinatorial Mathematics and Applications. University of North Carolina Press, Chapel Hill (1969).
12. Kennedy G.T., Pless V.: A coding-theoretic approach to extending designs. Discret. Math. **142**, 155–168 (1995).
13. Khosrovshahi G.B., Laue H.: t-designs with $t \geq 3$. In: Colbourn C.J., Dinitz J. (eds.) Handbook of Combinatorial Designs, pp. 79–101. CRC Press, New York (2007).
14. Kim J.-L., Pless V.: Designs in additive codes over GF(4). Des. Codes Cryptogr. **30**, 187–199 (2003).
15. MacWilliams F.J., Sloane N.J.A.: The Theory of Error-Correcting Codes. North-Holland, Amsterdam (1977).
16. Pless V.: Codes and designs—existence and uniqueness. Discret. Math. **92**, 261–274 (1991).
17. Reid C., Rosa A.: Steiner systems $S(2, 4)$—a survey. Electron. J. Comb. #DS18 (2010).
18. Tonchev V.D.: Quasi-symmetric designs, codes, quadrics, and hyperplane sections. Geom. Dedicata **48**, 295–308 (1993).
19. Tonchev V.D.: Codes and designs. In: Pless V.S., Huffman W.C. (eds.) Handbook of Coding Theory, vol. II, pp. 1229–1268. Elsevier, Amsterdam (1998).
20. Tonchev V.D.: Codes. In: Colbourn C.J., Dinitz J.H. (eds.) Handbook of Combinatorial Designs, 2nd edn, pp. 677–701. CRC Press, New York (2007).
21. van Lint J.H.: Introduction to Coding Theory, 3rd edn. Springer, New York (1999).