Cryptography and Communications (2021) 13:407–423
https://doi.org/10.1007/s12095-021-00472-4

Linear codes of 2-designs as subcodes of the generalized Reed-Muller codes

Zhiwen He[1] · **Jiejing Wen**[2,3]

Received: 9 August 2020 / Accepted: 8 January 2021 / Published online: 27 February 2021

Abstract
This paper is devoted to the affine-invariant ternary codes defined by Hermitian functions. We first compute the incidence matrices of the 2-designs supported by the minimum weight codewords of these ternary codes. Then we show that the linear codes spanned by the rows of these incidence matrices are subcodes of the 4-th order generalized Reed-Muller codes and also hold 2-designs. Finally, we determine the dimension and develop a lower bound on the minimum distance of the ternary linear codes.

Keywords Ternary code · 2-design · Incidence matrix · Generalized Reed-Muller code

Mathematics Subject Classification (2010) 94B15 · 05B05 · 51E10

1 Introduction

A t-design with parameters (n, k, λ) is a pair $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ with point set $\mathcal{P}$ and block set $\mathcal{B}$, where $\mathcal{P}$ has size n and each block in $\mathcal{B}$ is a k-subset of $\mathcal{P}$, such that any t points are contained in exactly λ blocks. We only consider simple designs, which are designs containing no repeated blocks, with $n > k > \lambda$. Let q be a prime power and $\mathbb{F}_q$ be the finite field of q elements. An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a k-dimensional linear subspace of the vector space $\mathbb{F}_q^n$ with minimum distance d. Let A_i, $0 \le i \le n$, denote the number of codewords of weight i in $\mathcal{C}$. The sequence $(A_0, A_1, \cdots, A_n)$ and $\sum_{i=0}^{n} A_i t^i$ are called the weight distribution and the weight enumerator of $\mathcal{C}$, respectively.

✉ Jiejing Wen
jjwen@sdu.edu.cn

Zhiwen He
zhiwen_he@zju.edu.cn

[1] School of Mathematical Sciences, Zhejiang University, Hangzhou 310027, China

[2] Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong University, Qingdao 266237, China

[3] School of Cyber Science and Technology, Shandong University, Qingdao 266237, China

The theories of t-designs and linear codes are closely related. Let $\mathbb{D} = (\mathcal{P}, \mathcal{B})$ be a t-(n, k, λ) design and let b be the number of blocks in $\mathcal{B}$. The incidence matrix $M_{\mathbb{D}} = (m_{ij})$ of $\mathbb{D}$ is a $b \times n$ matrix, where $m_{ij} = 1$, if the point p_j is in the block $B_i \in \mathcal{B}$ and $m_{ij} = 0$, otherwise. The rows of the incidence matrix $M_{\mathbb{D}}$ can be viewed as vectors of $\mathbb{F}_q^n$. Then the subspace $\mathcal{C}_q(\mathbb{D})$ spanned by these b vectors is called the linear code of $\mathbb{D}$ over $\mathbb{F}_q$. Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$ with each codeword indexed by the ordered elements $\{p_0, p_1, \cdots, p_{n-1}\}$. For any $A_i \neq 0$, we denote $\mathcal{B}_i$ as the collection of the supports $\mathrm{Suppt}(c) = \{p_j : c_{p_j} \neq 0, 0 \leq j \leq n-1\}$ for all $c = (c_{p_0}, c_{p_1}, \cdots, c_{p_{n-1}}) \in \mathcal{C}$ with weight i, $0 \leq i \leq n$. Let $\mathcal{P} = \{p_0, p_1, \cdots, p_{n-1}\}$. If the pair $(\mathcal{P}, \mathcal{B}_i)$ is a t-(n, i, λ) design for some positive integers λ and t, then we call it the support design of the code $\mathcal{C}$ and denote it by $\mathbb{D}_i(\mathcal{C})$.

It is known that t-designs and linear codes are closely related [3]. Many infinite families of 2-designs and 3-designs have been constructed from codes via different methods (see, e.g., [5–9, 12]). Recently, the 71-year-old open problem of the existence of an infinite family of linear codes holding 4-designs was solved by Tang and Ding [11]. But, it remains open whether there exists an infinite family of linear codes holding 5-designs. Ding, Tang and Tonchev recently studied the linear codes of 2-designs held in a class of affine-invariant ternary codes [4]. The ternary codes used in their paper are defined by the quadratic functions $\mathrm{Tr}(ax^2 + bx + c)$. In this paper, we consider the affine-invariant ternary codes defined by Hermitian functions, which are denoted by $\mathcal{C}(2m, 3)$. Let d denote the minimum distance of the code $\mathcal{C}(2m, 3)$, and let $\mathbb{D}_d(\mathcal{C}(2m, 3))$ denote the 2-design supported by the minimum weight codewords of $\mathcal{C}(2m, 3)$. The objective of this paper is to study the ternary codes $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$. The linear codes $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ are affine-invariant, that is, they also hold 2-designs. Moreover, the new linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ contains the original code $\mathcal{C}(2m, 3)$ as a subcode, and has many other affine-invariant subcodes. This implies that the structure of $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ is richer than the original code $\mathcal{C}(2m, 3)$. Furthermore, the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ is a subcode of the 4-th order ternary generalized Reed-Muller code.

The rest of this paper is organized as follows. In Section 2, we introduce some notation and basic results of cyclic codes, the generalized Reed-Muller codes, and the automorphism groups of linear codes. In Section 3, we consider the designs held in the affine-invariant ternary codes and the linear codes spanned by the rows of the incidence matrices of these designs. We present the vectors that spanned the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ in Theorems 3.3 and 3.4. We also determine the dimension and develop a lower bound on the minimum weight of $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$ in Theorem 3.5. In Section 4, we present proofs of our main results given in Section 3. In Section 5, we conclude this paper.

2 Preliminaries

2.1 Cyclic codes

An $[n, k, d]$ linear code $\mathcal{C}$ over $\mathbb{F}_q$ is a cyclic code if for each codeword $c = (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}$, the shifted codeword $(c_{n-1}, c_0, \cdots, c_{n-2})$ is also in $\mathcal{C}$. We define the residue class ring $\mathcal{R}_n[x] = \mathbb{F}_q[x]/(x^n - 1)$ and a subset $\mathcal{C}(x)$ of $\mathcal{R}_n[x]$ corresponding to the cyclic code $\mathcal{C}$

$$\mathcal{C}(x) = \{c_0 + c_1 x + \cdots + c_{n-1}x^{n-1} \in \mathcal{R}_n[x] : (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C}\}.$$

There is a bijection between the cyclic code $\mathcal{C}$ and the subset $\mathcal{C}(x)$ of $\mathcal{R}_n(x)$. It is easy to see that $xc(x) \in \mathcal{C}(x)$ for any $c(x) \in \mathcal{C}(x)$. Hence $\mathcal{C}(x)$ forms an ideal in the residue class ring $\mathcal{R}_n[x]$. Since $\mathcal{R}_n[x]$ is a principal ideal domain, $\mathcal{C}(x)$ is principal and $\mathcal{C}(x) = \langle g(x) \rangle$ for some monic polynomial $g(x) \in \mathcal{R}_n[x]$ with the smallest degree. We call $g(x)$ the generator polynomial and $h(x) = (x^n - 1)/g(x)$ the parity-check polynomial of $\mathcal{C}$. It is known that the dimension of the cyclic code $\mathcal{C}$ is $n - \deg(g(x))$ from Theorem 4.2.1 in [10].

Let n be an integer such that $\gcd(n, q) = 1$. The q-cyclotomic coset $C_s, 0 \leq s < n$, of s modulo n is defined by

$$C_s = \{s, sq, \cdots, sq^{r-1}\} (\mathrm{mod}\, n),$$

where r is the smallest positive integer such that $sq^r \equiv s \pmod{n}$. The smallest integer in C_s is called the coset leader of C_s. Note that these distinct q-cyclotomic cosets partition the set $\{0, 1, \cdots, n-1\}$. Let m be the order of q module n and γ be a primitive element of $\mathbb{F}_{q^m}$, i.e. $\mathbb{F}_{q^m}^* = \langle \gamma \rangle$. Let $\beta = \gamma^{\frac{q^m-1}{n}}$. Then β is a primitive n-th root of unity in $\mathbb{F}_{q^m}$. For each $s, 0 \leq s < n$, the minimal polynomial of β^s over $\mathbb{F}_q$ is $M_{\beta^s}(x) = \Pi_{i \in C_s}(x - \beta^i)$. The generator polynomial of the cyclic code $\mathcal{C}$ can be written as $g(x) = \Pi_{s \in S} M_{\beta^s}(x)$, where S is a collection of coset leaders of some cyclotomic cosets. We call the union of these cyclotomic cosets $T = \cup_{s \in S} C_s$ the defining set of $\mathcal{C}$. The roots of unity in $Z = \{\beta^i : i \in T\}$ are called zeros of the cyclic code $\mathcal{C}$ and $\{\beta^i : i \notin T\}$ are nonzeros of $\mathcal{C}$. We refer the reader to [10] for more details on cyclotomic cosets and minimal polynomials.

The dual code $\mathcal{C}^\perp$ of a linear code $\mathcal{C}$ is defined by

$$\mathcal{C}^\perp := \{c' \in \mathbb{F}_q^n \mid c \cdot c' = 0, \text{ for any } c \in \mathcal{C}\},$$

where $\cdot$ denotes the inner product. If $\mathcal{C}$ is a cyclic code with the parity-check polynomial $h(x)$, then $\mathcal{C}^\perp$ has the generator polynomial $x^k h(x^{-1})/h(0)$, where $k = \deg(h(x))$.

The following theorem from [10] shows that the zeros of $\mathcal{C}^\perp$ can be derived from the nonzeros of $\mathcal{C}$.

Theorem 2.1 [10, Theorem 4.4.9] *Let $\mathcal{C}$ be an $[n, k, d]$ cyclic code over $\mathbb{F}_q$. If $\gamma_1, \cdots, \gamma_k$ are the nonzeros of $\mathcal{C}$, then $\gamma_1^{-1}, \cdots, \gamma_k^{-1}$ are the zeros of $\mathcal{C}^\perp$.*

Proposition 2.2 [10, Section 4.4] *Let $\mathcal{C}_i$ be cyclic codes of length n over $\mathbb{F}_q$ with defining sets T_i for $1 \leq i \leq 2$. Then the linear code $\mathcal{C}_1 + \mathcal{C}_2 = \{c_1 + c_2 \mid c_i \in \mathcal{C}_i, 1 \leq i \leq 2\}$ has defining set $T_1 \cap T_2$.*

The extended code of a linear code $\mathcal{C}$ is defined by

$$\overline{\mathcal{C}} = \{(c_0, c_1, \cdots, c_n) \in \mathbb{F}_q^{n+1} \mid (c_0, c_1, \cdots, c_{n-1}) \in \mathcal{C} \text{ such that } \sum_{i=0}^{n} c_i = 0\}.$$

If H is the parity check matrix of $\mathcal{C}$, then the parity check matrix of $\overline{\mathcal{C}}$ is

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

where $\mathbf{1} = (1, 1, \cdots, 1)$ and $\mathbf{0} = (0, 0, \cdots, 0)^\top$.

Theorem 2.3 [10, Theorem 4.4.19] *Let n be a positive integer and q be a prime power. Let $g(x)$ be an irreducible factor of $x^n - 1$ over $\mathbb{F}_q$ with degree s. Assume that*

$\gamma \in \mathbb{F}_{q^s}$ is a root of $g(x)$. Let $\mathrm{Tr}_s : \mathbb{F}_{q^s} \to \mathbb{F}_q$ be the trace map from $\mathbb{F}_{q^s}$ to $\mathbb{F}_q$. Then

$$\mathcal{C}_\gamma = \left\{ \sum_{i=0}^{n-1} \mathrm{Tr}_s(a\gamma^i)x^i | a \in \mathbb{F}_{q^s} \right\}$$

is an $[n, s]$ irreducible cyclic code with nonzeros $\{\gamma^{-q^i} | 0 \le i < s\}$.

2.2 The generalized Reed-Muller codes

Let q be a prime power and l, m be positive integers with $1 \le l < (q-1)m$. The l-th order punctured generalized Reed-Muller code $\mathcal{R}_q(l, m)^*$ over $\mathbb{F}_q$ is the cyclic code of length $n = q^m - 1$ with generator polynomial

$$g(x) = \prod_{\substack{1 \le i \le n-1 \\ w_q(i) < (q-1)m-l}} (x - \gamma^i),$$

where γ is a primitive element of $\mathbb{F}_{q^m}$, $i = \sum_{j=0}^{m-1} i_j q^j$ with $0 \le i_j \le q-1$ and $w_q(i) = \sum_{i=0}^{m-1} i_j$.

Assmus and Key [1] provided the following parameters of the punctured generalized Reed-Muller code $\mathcal{R}_q(l, m)^*$.

Theorem 2.4 [1, Section 5] *The code $\mathcal{R}_q(l, m)^*$ has length $n = q^m - 1$, dimension*

$$k = \sum_{i=0}^{l} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq}$$

and minimum weight $d = (q - l_0)q^{m-l_1-1} - 1$, where $l = l_1(q-1) + l_0$ and $0 \le l_0 < q - 1$.

The dual of the punctured generalized Reed-Muller code $(\mathcal{R}_q(l, m)^*)^\perp$ and its parameters are obtained in [1] and [2].

Theorem 2.5 [1, Corollary 5.21] *The code $(\mathcal{R}_q(l, m)^*)^\perp$ is the cyclic code with generator polynomial*

$$g^\perp(x) = \prod_{\substack{1 \le i \le n-1 \\ \omega_q(i) < l}} (x - \gamma^i).$$

Theorem 2.6 [2, Section 5.4] *The code $(\mathcal{R}_q(l, m)^*)^\perp$ has length $n = q^m - 1$, dimension*

$$k^\perp = n - \sum_{i=0}^{l} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq},$$

and minimum weight

$$d^\perp \ge (q - l_0')q^{m-l_1'-1},$$

where $m(q-1) - 1 - l = l_1'(q-1) + l_0'$ and $0 \le l_0' < q - 1$.

The generalized Reed-Muller code $\mathcal{R}_q(l, m)$ is the extended code of the punctured generalized Reed-Muller code $\mathcal{R}_q(l, m)^*$.

Theorem 2.7 [1, Section 5] *The code $\mathcal{R}_q(l, m)$ has length $n = q^m$, dimension*

$$k = \sum_{i=0}^{l} \sum_{j=0}^{m} (-1)^j \binom{m}{j} \binom{i - jq + m - 1}{i - jq}$$

and minimum weight $d = (q - l_0)q^{m-l_1-1}$, where $l = l_1(q - 1) + l_0$ and $0 \le l_0 < q - 1$.

2.3 Automorphism groups of linear codes

Let $\mathcal{C}$ be an $[n, k, d]$ linear code over $\mathbb{F}_q$. The set of coordinate permutations that maps $\mathcal{C}$ to itself forms a subgroup of the symmetric group $\mathrm{Sym}(n)$. We call this set the permutation automorphism group of $\mathcal{C}$ and denote it by $\mathrm{PAut}(\mathcal{C})$. A monomial matrix over $\mathbb{F}_q$ is a square matrix such that each row and column have exactly one nonzero element of $\mathbb{F}_q$. The collection of all monomial matrix that maps $\mathcal{C}$ to itself forms a group denoted by $\mathrm{MAut}(\mathcal{C})$, which is called the monomial automorphism group of $\mathcal{C}$. By definition, every element of $\mathrm{MAut}(\mathcal{C})$ can be expressed as DP or PD_1, where D and D_1 are diagonal matrices and P is a permutation matrix. All permutations of the form $DP\gamma$ fixing $\mathcal{C}$ form a group, called the automorphism group of $\mathcal{C}$ and denoted by $\mathrm{Aut}(\mathcal{C})$, where γ is an automorphism of $\mathbb{F}_q$. By definition, we have $\mathrm{PAut}(\mathcal{C}) \subseteq \mathrm{MAut}(\mathcal{C}) \subseteq \mathrm{Aut}(\mathcal{C})$. The automorphism group $\mathrm{Aut}(\mathcal{C})$ is called t-transitive if for any two ordered t-subsets A and B of the set of coordinates of the codewords in $\mathcal{C}$, there exists an element $DP\gamma \in \mathrm{Aut}(\mathcal{C})$ such that P maps A to B.

The following theorem is a sufficient condition for a linear code $\mathcal{C}$ to hold t-designs.

Theorem 2.8 [10, Theorem 8.4.7] *Let $\mathcal{C}$ be a code of length n over $\mathbb{F}_q$. If $\mathrm{Aut}(\mathcal{C})$ is t-transitive, then for any integer i with $i \ge t$, the codewords of weight i hold a t-design.*

The general affine group $\mathrm{GA}_1(\mathbb{F}_{q^m})$ is the set of permutations of $\mathbb{F}_{q^m}$:

$$\{\sigma_{s_1,s_2} : s_1 \in \mathbb{F}_{q^m}^*, s_2 \in \mathbb{F}_{q^m}\},$$

where $\sigma_{s_1,s_2}(x) = s_1x + s_2$ for any $x \in \mathbb{F}_{q^m}$. Let $\mathcal{C}$ be a linear code of length q^m over $\mathbb{F}_q$. We index the codewords of $\mathcal{C}$ by the elements of $\mathbb{F}_{q^m}$. The linear code $\mathcal{C}$ is called affine invariant if the general affine group $\mathrm{GA}_1(\mathbb{F}_{q^m})$ leaves $\mathcal{C}$ invariant, i.e. $\mathrm{GA}_1(\mathbb{F}_{q^m}) \le \mathrm{PAut}(\mathcal{C})$. It is well known that $\mathrm{GA}_1(\mathbb{F}_{q^m})$ is doubly transitive on $\mathbb{F}_{q^m}$. Then the following theorem follows from Theorem 2.8.

Theorem 2.9 [3, Theorem 6.6] *Let A_i be the number of codewords of weight i for $0 \le i \le n$. If the linear code $\mathcal{C}$ is affine invariant, then for each i with $A_i \ne 0$, the supports of the codewords of weight i in $\mathcal{C}$ form a 2-design.*

3 Codes of designs held in a class of affine-invariant ternary codes

Let $m \ge 2$ be a positive integer and let p be an odd prime. Denote Tr_s as the trace map from $\mathbb{F}_{p^s}$ to $\mathbb{F}_p$. We consider the linear code

$$\mathcal{C}(2m, p) = \{c(a, b, h) \mid a \in \mathbb{F}_{p^m}, b \in \mathbb{F}_{p^{2m}}, h \in \mathbb{F}_p\}, \tag{3.1}$$

where

$$c(a, b, h) = (\mathrm{Tr}_{2m}(at^{p^m+1} + bt) + h)_{t \in \mathbb{F}_{p^{2m}}}.$$

As shown in [9], the code $\mathcal{C}(2m, p)$ is affine invariant, thus it holds 2-designs. For each codeword $c(a, b, h)$ in $\mathcal{C}(2m, p)$, the Hamming weight $w_H(c(a, b, h)) = p^{2m} - T(a, b, h)$, where

$$T(a, b, h) = |\{t \in \mathbb{F}_{p^{2m}} \mid \mathrm{Tr}_{2m}(at^{p^m+1} + bt) + h = 0\}|. \tag{3.2}$$

Lemma 3.1 [9] *Let $T(a, b, h)$ be defined in (3.2) for $a \in \mathbb{F}_{p^m}$, $b \in \mathbb{F}_{p^{2m}}$ and $h \in \mathbb{F}_p$. Then*

(1) If $a = b = h = 0$, then $T(a, b, h) = p^{2m}$.

(2) If $a = b = 0$ and $h \neq 0$, then $T(a, b, h) = 0$.

(3) If $a = 0$ and $b \neq 0$, then $T(a, b, h) = p^{2m-1}$.

(4) If $a \neq 0$, then

$$T(a, b, h) = \begin{cases} p^{2m-1} - p^{m-1}(p-1) & \text{if } h = \mathrm{Tr}_{2m}(as_{at,bt}^{p^m+1}), \\ p^{2m-1} + p^{m-1} & \text{if } h \neq \mathrm{Tr}_{2m}(as_{at,bt}^{p^m+1}), \end{cases}$$

where $t \in \mathbb{F}_p^*$ and $s_{at,bt}^{p^m+1}$ is a solution of $((at)^{p^m} + at)s = 2ats = -(bt)^{p^m}$, i.e. $s_{at,bt}^{p^m+1} = -2^{-1}a^{-1}b^{p^m}t^{p^m-1} = -2^{-1}a^{-1}b^{p^m}$.

Then a codeword $c(a, b, h)$ has minimum weight $d = p^{2m-1}(p-1) - p^{m-1}$ only if $a \in \mathbb{F}_{p^m}^*$, $b \in \mathbb{F}_{p^{2m}}$ and $h \in \mathbb{F}_p \setminus \{\mathrm{Tr}_{2m}(-2^{-1}b)\}$. The linear code $\mathcal{C}(2m, p)$ has parameters $[p^{2m}, 3m+1, p^{2m-1}(p-1) - p^{m-1}]$ and the weight distribution in Table 1, as stated in Theorem 3 of [9]. Let $\mathbb{D}_d(\mathcal{C}(2m, p))$ be the support design of the code $\mathcal{C}(2m, p)$, in which the blocks are the supports of the codewords in $\mathcal{C}(2m, p)$ with minimum weight d. We know that $\mathbb{D}_d(\mathcal{C}(2m, p))$ is a 2-design from [9]. Let $M_{\mathbb{D}_d}$ be the incidence matrix of $\mathbb{D}_d(\mathcal{C}(2m, p))$ and $\mathcal{C}_p(\mathbb{D}_d(\mathcal{C}(2m, p)))$ be the linear code spanned by the rows of $M_{\mathbb{D}_d}$ over $\mathbb{F}_p$. We will restrict ourselves to the case of $p = 3$ and compute the dimension and the minimum weight of $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m, 3)))$.

Remark 3.2 The ternary linear code defined by the quadratic functions $\mathrm{Tr}_{2m}(at^2 + bt) + h$ over $\mathbb{F}_3$ and treated in [4] has parameters $[3^{2m}, 4m+1, 2(3^{2m-1} - 3^{m-1})]$. The ternary linear code defined by the Hermitian functions $\mathrm{Tr}_{2m}(at^{3^m+1} + bt) + h$ over $\mathbb{F}_3$ in (3.1) has parameters $[n, k, d] = [3^{2m}, 3m+1, 2 \cdot 3^{2m-1} - 3^{m-1}]$. Hence they are not equivalent, as they have different dimensions.

To simplify notation, we identify $f(t)$ with the vector $(f(t))_{t \in \mathbb{F}_{3^{2m}}}$ below. In the following, we present our main results whose proofs will be given in Section 4.

Table 1 The weight distribution of $\mathcal{C}(2m, p)$

Weight	Multiplicity
0	1
$p^{2m-1}(p-1) - p^{m-1}$	$p^{2m}(p^m - 1)(p-1)$
$p^{2m-1}(p-1)$	$p(p^{2m} - 1)$
$(p^{2m-1} + p^{m-1})(p-1)$	$p^{2m}(p^m - 1)$
p^{2m}	$p - 1$

Theorem 3.3 *For any integer $m \geq 2$, the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ over $\mathbb{F}_3$ is generated by*

$$\left\{ \begin{array}{c} \mathrm{Tr}_{2m}(bt), \mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't), \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt), \\ \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1}), \mathrm{Tr}_{2m}(at^{3^m+1}), 1 \mid a, a' \in \mathbb{F}_{3^m}, b, b' \in \mathbb{F}_{3^{2m}} \end{array} \right\}.$$

Theorem 3.4 *For any integer $m \geq 2$, the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is given by*

$$\left\{ \begin{array}{c} \sum_{i=0}^{m-1} \mathrm{Tr}_{2m}(b_i t^{(3^m+1)3^i+1}) + \sum_{i=0}^{2m-1} \mathrm{Tr}_{2m}(b'_i t^{3^i+1}) \\ + \sum_{i=0}^{m-1} \mathrm{Tr}_m(a_i t^{(3^m+1)(3^i+1)}) + \mathrm{Tr}_{2m}(bt) + h : b, b_i, b'_i \in \mathbb{F}_{3^{2m}}, a_i \in \mathbb{F}_{3^m}, h \in \mathbb{F}_3 \end{array} \right\},$$

and it holds 2-designs.

Theorem 3.5 *For any integer $m \geq 1$, the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ has length $n = p^{2m}$, dimension $k = \frac{9m^2+7m}{2} + 1$ and the lower bound 3^{2m-2} on the minimum distance.*

Example 3.6 The parameters of the linear code $\mathcal{C}(2m,3)$ and $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ for $m = 1, 2$ are listed as follows:

m	$\mathcal{C}(2m,3)$	$\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$
1	[9, 4, 5]	[9, 9, 1]
2	[81, 7, 51]	[81, 26, 21].

The linear code $\mathcal{C}(4,3)$ has weight distribution

$$1 + 1296z^{51} + 240z^{54} + 648z^{60} + 2z^{81}.$$

The linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(4,3)))$ has weight distribution

$$\begin{array}{lllll} 1 & +648z^{21} & +240z^{27} & +38880z^{28} & +25920z^{29} \\ +104976z^{30} & +373248z^{31} & +678780z^{32} & +2491560z^{33} & +9305280z^{34} \\ +12791520z^{35} & +52067880z^{36} & +167585760z^{37} & +193771440z^{38} & +633582000z^{39} \\ +1789957440z^{40} & +1784204820z^{41} & +5114657520z^{42} & +12311494560z^{43} & +10655818920z^{44} \\ +26240268600z^{45} & +54869931360z^{46} & +40818498480z^{47} & +86821798860z^{48} & +155822087880z^{49} \\ +99765111888z^{50} & +181835828208z^{51} & +279785262240z^{52} & +153082363320z^{53} & +238171803600z^{54} \\ +311801503680z^{55} & +144740601000z^{56} & +190453223160z^{57} & +210148421760z^{58} & +81951931440z^{59} \\ +90132625584z^{60} & +82728913248z^{61} & +26672379840z^{62} & +24134094720z^{63} & +18117430380z^{64} \\ +4739847840z^{65} & +3450820320z^{66} & +2053913760z^{67} & +424174320z^{68} & +238097880z^{69} \\ +109483488z^{70} & +16715808z^{71} & +7076700z^{72} & +2442960z^{73} & +116640z^{74} \\ +58320z^{75} & +38880z^{77} & +6480z^{78} & +2106z^{80} & +2186z^{81}. \end{array}$$

4 Proofs of the main results

In this section, we prove Theorems 3.3, 3.4 and 3.5. We first compute the rows of the incidence matrix $M_{\mathbb{D}_d}$ of $\mathbb{D}_d(\mathcal{C}(2m,3))$ and list the result in Theorem 3.3. Next, we simplify the form of these rows and give the proof of Theorem 3.4. The results in Theorem 3.4 imply that the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is a subcode of the 4-th order generalized Reed-Muller code. It induces the lower bound of the minimum weight of the code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. Finally, we get the dimension of the code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ by calculating the size of the defining set of $\mathcal{C}$ defined in (4.12) and state the proof of Theorem 3.5.

We can easily get the following lemma from the definition of $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ in Section 3.

Lemma 4.1 *Let $m \geq 2$ be a positive integer. The linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ defined as above is generated by the vectors in the following set over $\mathbb{F}_3$:*

$$\{(\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h)^2 \mid a \in \mathbb{F}_{3^m}^*, b \in \mathbb{F}_{3^{2m}}, h \in \mathbb{F}_3 \setminus \{\mathrm{Tr}_{2m}(b)\}\}.$$

Using Lemma 4.1, for any $a \in \mathbb{F}_{3^m}^*$, $b \in \mathbb{F}_{3^{2m}}$, $h \in \mathbb{F}_3 \setminus \{\mathrm{Tr}_{2m}(b)\}$, we have

$$\begin{aligned}(\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h)^2 &= \mathrm{Tr}_{2m}(at^{3^m+1}+bt)^2 + 2h\mathrm{Tr}_{2m}(at^{3^m+1}+bt)+h^2 \\ &= \mathrm{Tr}_{2m}(at^{3^m+1})^2 + 2\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) + \mathrm{Tr}_{2m}(bt)^2 \\ &\quad +2h\mathrm{Tr}_{2m}(at^{3^m+1}) + 2h\mathrm{Tr}_{2m}(bt) + h^2 \ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))),\end{aligned} \tag{4.1}$$

$$\begin{aligned}(\mathrm{Tr}_{2m}(at^{3^m+1}-bt)+h)^2 &= \mathrm{Tr}_{2m}(at^{3^m+1}-bt)^2 + 2h\mathrm{Tr}_{2m}(at^{3^m+1}-bt)+h^2 \\ &= \mathrm{Tr}_{2m}(at^{3^m+1})^2 - 2\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) + \mathrm{Tr}_{2m}(bt)^2 \\ &\quad +2h\mathrm{Tr}_{2m}(at^{3^m+1}) - 2h\mathrm{Tr}_{2m}(bt) + h^2 \ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).\end{aligned} \tag{4.2}$$

Subtracting (4.1) from (4.2), we obtain that

$$\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) + h\mathrm{Tr}_{2m}(bt) \ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.3}$$

Adding (4.1) to (4.2), we get that

$$2\mathrm{Tr}_{2m}(at^{3^m+1})^2 + 2\mathrm{Tr}_{2m}(bt)^2 + h\mathrm{Tr}_{2m}(at^{3^m+1}) + 2h^2 \ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \tag{4.4}$$

We show that each item of (4.1) is also in $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

Lemma 4.2 *Let $a \in \mathbb{F}_{3^m}$ and $b \in \mathbb{F}_{3^{2m}}$, then $\{\mathrm{Tr}_{2m}(bt), \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt)\} \subseteq \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.*

Proof For any $a \in \mathbb{F}_{3^m}^*$, $b \in \mathbb{F}_{3^{2m}}$ and $h_1 \neq h_2 \in \mathbb{F}_3 \setminus \{\mathrm{Tr}_{2m}(b)\}$, we have

$$\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) + h_1\mathrm{Tr}_{2m}(bt) \ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \tag{4.5}$$

$$\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) + h_2\mathrm{Tr}_{2m}(bt) \ \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))) \tag{4.6}$$

by (4.3). The result is easily obtained by subtracting (4.5) from (4.6). □

Lemma 4.3 *For any $t \in \mathbb{F}_{3^{2m}}$, the following equations hold:*

(1) $\sum_{a\in\mathbb{F}_{3^m}^*} \mathrm{Tr}_{2m}(at^{3^m+1})^2 = 0.$

(2) $\sum_{b\in\mathbb{F}_{3^{2m}}^*} \mathrm{Tr}_{2m}(bt)^2 = 0.$

(3) $\sum_{a\in\mathbb{F}_{3^m}^*} \mathrm{Tr}_{2m}(at^{3^m+1}) = 0.$

Proof The conclusions are obvious if $t = 0$. We now assume that $t \neq 0$. For any $t \in \mathbb{F}_{3^{2m}}^*$, the equation $(t^{3^m+1})^{3^m} = t^{3^m+1}$ implies that $t^{3^m+1} \in \mathbb{F}_{3^m}^*$. Note that $\mathrm{Tr}_{2m}(a) = 2\mathrm{Tr}_m(a)$ for any $a \in \mathbb{F}_{3^m}$.

Firstly, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_{2m}(at^{3^m+1})^2 &= \sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_m(a)^2\\ &= |\{a\in\mathbb{F}_{3^m}|\mathrm{Tr}_m(a)\neq 0\}|(\bmod 3)\\ &= 3^m-|\{a\in\mathbb{F}_{3^m}|\mathrm{Tr}_m(a)=0\}|(\bmod 3)\\ &= 3^m-3^{m-1}(\bmod 3)\\ &= 0.\end{aligned}$$

Secondly, we have

$$\begin{aligned}\sum_{b\in\mathbb{F}_{3^{2m}}^*}\mathrm{Tr}_{2m}(bt)^2 &= \sum_{b\in\mathbb{F}_{3^{2m}}}\mathrm{Tr}_{2m}(b)^2\\ &= |\{b\in\mathbb{F}_{3^{2m}}|\mathrm{Tr}_{2m}(b)\neq 0\}|(\bmod 3)\\ &= 3^{2m}-3^{2m-1}(\bmod 3)\\ &= 0.\end{aligned}$$

Finally, we have

$$\begin{aligned}\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_{2m}(at^{3^m+1}) &= 2\sum_{a\in\mathbb{F}_{3^m}^*}\mathrm{Tr}_m(a)\\ &= 2\mathrm{Tr}_m(\sum_{a\in\mathbb{F}_{3^m}^*}a)\\ &= 0.\end{aligned}$$

□

Lemma 4.4 *The constant codeword* $1\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

Proof For any $a\in\mathbb{F}_{3^m}^*$ and $b\in\mathbb{F}_{3^{2m}}$, we choose $h_b=\mathrm{Tr}_{2m}(b)+1$. It follows from Lemma 4.3 and (4.4) that

$$\begin{aligned}&\sum_{b\in\mathbb{F}_{3^{2m}}^*}\sum_{a\in\mathbb{F}_{3^m}^*}(\mathrm{Tr}_{2m}(at^{3^m+1})^2+\mathrm{Tr}_{2m}(bt)^2+2h_b\mathrm{Tr}_{2m}(at^{3^m+1})+h_b^2)\\ &\quad= 2\sum_{b\in\mathbb{F}_{3^{2m}}^*}(\mathrm{Tr}_{2m}(b)+1)^2\\ &\quad= \sum_{b\in\mathbb{F}_{3^{2m}}^*}(\mathrm{Tr}_{2m}(b)+2)\\ &\quad= 1\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).\end{aligned}$$

□

Lemma 4.5 *Let* $b,b'\in\mathbb{F}_{3^{2m}}$, *then* $\mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't)\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$.

Proof Let $b_1=\frac{b+b'}{2}$, $b_2=\frac{b'-b}{2}\in\mathbb{F}_{3^{2m}}$. Plugging b_1,b_2 into (4.4), we obtain

$$2\mathrm{Tr}_{2m}(at^{3^m+1})^2+2\mathrm{Tr}_{2m}(b_1t)^2+h_1\mathrm{Tr}_{2m}(at^{3^m+1})+2h_1^2\in\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))),\quad(4.7)$$

$$2\mathrm{Tr}_{2m}(at^{3^m+1})^2 + 2\mathrm{Tr}_{2m}(b_2t)^2 + h_2\mathrm{Tr}_{2m}(at^{3^m+1}) + 2h_2^2 \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \quad (4.8)$$

where $h_1 \in \mathbb{F}_3 \setminus \{\mathrm{Tr}(b_1)\}$ and $h_2 \in \mathbb{F}_3 \setminus \{\mathrm{Tr}(b_2)\}$. We set $h_1 = h_2 = h$ for some $h \in \mathbb{F}_3 \setminus \{\mathrm{Tr}_{2m}(b_1), \mathrm{Tr}_{2m}(b_2)\}$. Then subtracting (4.8) from (4.7), we get

$$2\mathrm{Tr}_{2m}((b_1 - b_2)t)\mathrm{Tr}_{2m}((b_1 + b_2)t) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).$$

Hence, $\mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. □

Lemma 4.6 *Let $a, a' \in \mathbb{F}_{3^m}$, then we have*

$$\{\mathrm{Tr}_{2m}(at^{3^m+1}), \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1})\} \subseteq \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).$$

Proof By Lemma 4.4, Lemma 4.5 and (4.4), we have

$$\mathrm{Tr}_{2m}(at^{3^m+1})^2 + 2h\mathrm{Tr}_{2m}(at^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \quad (4.9)$$

We can choose $h_1 \neq h_2 \in \mathbb{F}_3 \setminus \{\mathrm{Tr}_{2m}(b)\}$ and plug h_1, h_2 into (4.9), we then obtain

$$\mathrm{Tr}_{2m}(at^{3^m+1})^2 + 2h_1\mathrm{Tr}_{2m}(at^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))), \quad (4.10)$$

$$\mathrm{Tr}_{2m}(at^{3^m+1})^2 + 2h_2\mathrm{Tr}_{2m}(at^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))). \quad (4.11)$$

Subtracting (4.11) from (4.10), we arrive at

$$2(h_1 - h_2)\mathrm{Tr}_{2m}(at^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).$$

We then deduce that $\mathrm{Tr}_{2m}(at^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ and $\mathrm{Tr}_{2m}(at^{3^m+1})^2 \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. Let $a_1 = \frac{a+a'}{2}$, $a_2 = \frac{a-a'}{2} \in \mathbb{F}_{3^m}$. Note that $\mathrm{Tr}_{2m}(a_1t^{3^m+1})^2, \mathrm{Tr}_{2m}(a_2t^{3^m+1})^2 \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. So we have

$$\begin{aligned}\mathrm{Tr}_{2m}(a_1t^{3^m+1})^2 - \mathrm{Tr}_{2m}(a_2t^{3^m+1})^2 &= \mathrm{Tr}_{2m}((a_1+a_2)t^{3^m+1})\mathrm{Tr}_{2m}((a_1-a_2)t^{3^m+1}) \\ &= \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).\end{aligned}$$

□

Proof of Theorem 3.3 The desired result is an easy consequence of the results above and (4.1). □

Lemma 4.7 [13, Corollary 8.4] *Let p be a prime and n a positive integer. Let $t_1, \cdots, t_n \in \mathbb{F}_{p^n}$. Then $\{t_1, \cdots, t_n\}$ is a basis of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$ if and only if*

$$\begin{vmatrix} t_1 & t_2 & \cdots & t_n \\ t_1^p & t_2^p & \cdots & t_n^p \\ \vdots & \vdots & \cdots & \vdots \\ t_1^{p^{n-1}} & t_2^{p^{n-1}} & \cdots & t_n^{p^{n-1}} \end{vmatrix} \neq 0.$$

Lemma 4.8 *For any positive integer $m \geq 2$, we have*

$$\langle \mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) \mid b, b' \in \mathbb{F}_{3^{2m}} \rangle = \left\langle \sum_{i=0}^{2m-1} \mathrm{Tr}_{2m}(b_it^{3^i+1}) \mid b_i \in \mathbb{F}_{3^{2m}} \right\rangle.$$

Proof For any $b, b' \in \mathbb{F}_{3^{2m}}$,

$$\begin{aligned}\mathrm{Tr}_{2m}(bt)\mathrm{Tr}_{2m}(b't) &= \sum_{i=0}^{2m-1}\sum_{j=0}^{2m-1} b^{3^i} b'^{3^j} t^{3^i+3^j} = \sum_{i=0}^{2m-1} b^{3^i}\left(\sum_{j=0}^{2m-1} b'^{3^{j-i}} t^{1+3^{j-i}}\right)^{3^i} \\ &= \sum_{i=0}^{2m-1} b^{3^i}\left(\sum_{j=0}^{2m-1} b'^{3^j} t^{1+3^j}\right)^{3^i} = \sum_{j=0}^{2m-1} \mathrm{Tr}_{2m}(bb'^{3^j} t^{1+3^j}).\end{aligned}$$

Let γ be a primitive element of $\mathbb{F}_{3^{2m}}$. Then $\{\gamma, \gamma^3, \cdots, \gamma^{3^{2m-1}}\}$ forms a normal basis of $\mathbb{F}_{3^{2m}}$ over $\mathbb{F}_3$. By Lemma 4.7, the elements in

$$\{(b', b'^3, \cdots, b'^{3^{2m-1}}) \mid b' = \gamma^{3^i}, 0 \le i \le 2m-1\}$$

are linear independently over $\mathbb{F}_3$ which means that they form a basis of $\mathbb{F}_{3^{2m}}^{2m}$ over $\mathbb{F}_{3^{2m}}$. Hence $\langle \sum_{j=0}^{2m-1} \mathrm{Tr}_{2m}(bb'^{3^j} t^{3^j+1}) \mid b, b' \in \mathbb{F}_{3^{2m}}\rangle = \langle \sum_{i=0}^{2m-1} \mathrm{Tr}_{2m}(b_i t^{3^i+1}) \mid b_i \in \mathbb{F}_{3^{2m}}\rangle$. □

Lemma 4.9 *For any positive integer $m \ge 2$, we have*

$$\langle \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) \mid a \in \mathbb{F}_{3^m}, b \in \mathbb{F}_{3^{2m}}\rangle = \left\langle \sum_{i=0}^{m-1} \mathrm{Tr}_{2m}(b_i t^{(3^m+1)3^i+1}) \mid b_i \in \mathbb{F}_{3^{2m}} \right\rangle.$$

Proof For any $a \in \mathbb{F}_{3^m}$ and $b \in \mathbb{F}_{3^{2m}}$,

$$\begin{aligned}\mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(bt) &= 2\sum_{i=0}^{m-1}\left(at^{3^m+1}\right)^{3^i}\sum_{j=0}^{2m-1}(bt)^{3^j} = 2\sum_{j=0}^{2m-1}(bt)^{3^j}\sum_{i=0}^{m-1}(at^{3^m+1})^{3^{i+j}} \\ &= 2\sum_{j=0}^{2m-1}\left(bt\sum_{i=0}^{m-1}\left(at^{3^m+1}\right)^{3^i}\right)^{3^j} = 2\sum_{i=0}^{m-1}\mathrm{Tr}_{2m}\left(ba^{3^i}t^{(3^m+1)3^i+1}\right).\end{aligned}$$

By Lemma 4.7, the elements in

$$\left\{\left(a, a^3, \cdots, a^{3^{m-1}}\right) \mid a = \gamma^{(3^m+1)3^i}, 0 \le i \le m-1\right\}$$

are linear independently over $\mathbb{F}_3$ which means that they form a basis of $\mathbb{F}_{3^{2m}}^m$ over $\mathbb{F}_{3^{2m}}$. Hence $\langle 2\sum_{i=0}^{m-1} \mathrm{Tr}_{2m}(ba^{3^i}t^{(3^m+1)3^i+1}) \mid a \in \mathbb{F}_{3^m}, b \in \mathbb{F}_{3^{2m}}\rangle = \langle \sum_{i=0}^{m-1} \mathrm{Tr}_{2m}(b_i t^{(3^m+1)3^i+1}) \mid b_i \in \mathbb{F}_{3^{2m}}\rangle$. □

Lemma 4.10 *For any positive integer $m \ge 2$, we have*

$$\langle \mathrm{Tr}_{2m}(at^{3^m+1})\mathrm{Tr}_{2m}(a't^{3^m+1}) \mid a, a' \in \mathbb{F}_{3^m}\rangle = \left\langle \sum_{i=0}^{m-1} \mathrm{Tr}_m\left(a_i t^{(3^m+1)(3^i+1)}\right) \mid a_i \in \mathbb{F}_{3^m} \right\rangle.$$

Proof For any $a, a' \in \mathbb{F}_{3^m}$,

$$\begin{aligned}\mathrm{Tr}_{2m}(a't^{3^m+1})\mathrm{Tr}_{2m}(at^{3^m+1}) &= \sum_{i=0}^{2m-1}\left(a't^{3^m+1}\right)^{3^i}\sum_{j=0}^{2m-1}\left(at^{3^m+1}\right)^{3^j} = \sum_{i=0}^{2m-1}\left(\left(a't^{3^m+1}\right)\sum_{j=0}^{2m-1}\left(at^{3^m+1}\right)^{3^{j-i}}\right)^{3^i}\\ &= \sum_{i=0}^{2m-1}\left(\left(a't^{3^m+1}\right)\sum_{j=0}^{2m-1}\left(at^{3^m+1}\right)^{3^j}\right)^{3^i} = \sum_{i=0}^{2m-1}\left(\sum_{j=0}^{2m-1}a'a^{3^j}t^{(3^m+1)(3^j+1)}\right)^{3^i}\\ &= \sum_{j=0}^{2m-1}\mathrm{Tr}_{2m}\left(a'a^{3^j}t^{(3^m+1)(3^j+1)}\right) = \sum_{j=0}^{m-1}\mathrm{Tr}_m\left(a'a^{3^j}t^{(3^m+1)(3^j+1)}\right).\end{aligned}$$

Similar to the proof in Lemma 4.9, we have $\langle\sum_{j=0}^{m-1}\mathrm{Tr}_m(a'a^{3^j}t^{(3^m+1)(3^j+1)}) \mid a, a' \in \mathbb{F}_{3^m}\rangle = \langle\sum_{i=0}^{m-1}\mathrm{Tr}_m(a_it^{(3^m+1)(3^i+1)}) \mid a_i \in \mathbb{F}_{3^m}\rangle$. □

Proof of Theorem 3.4 The first part of the theorem follows from Theorem 3.3 and Lemmas 4.8−4.10.

Now we prove that the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is affine invariant and it then holds 2-designs by Theorem 2.9. For any $\sigma_{s_1,s_2} \in \mathrm{GA}_1(\mathbb{F}_{3^{2m}})$ with $s_1 \in \mathbb{F}_{3^{2m}}^*$ and $s_2 \in \mathbb{F}_{3^{2m}}$, we only need to show that $\mathrm{Tr}_{2m}(b\sigma_{s_1,s_2}(t) + b'(\sigma_{s_1,s_2}(t))^{3^i+1} + b''(\sigma_{s_1,s_2}(t))^{(3^m+1)3^j+1} + c(\sigma_{s_1,s_2}(t))^{(3^m+1)(3^k+1)}) + h \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ for all $0 \le i \le 2m-1, 0 \le j,k \le m-1$, $b, b', b'' \in \mathbb{F}_{3^{2m}}$, $c \in \mathbb{F}_{3^m}$ and $h \in \mathbb{F}_3$. It is easy to check that $\mathrm{Tr}_{2m}(b(s_1t+s_2) + b'(s_1t+s_2)^{3^i+1}) + h \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. We get that

$$\begin{aligned}\mathrm{Tr}_{2m}(b''(s_1t+s_2)^{(3^m+1)3^j+1}) &= \mathrm{Tr}_{2m}(b''(s_1^{3^{m+j}}t^{3^{m+j}} + s_2^{3^{m+j}})(s_1^{3^j}t^{3^j} + s_2^{3^j})(s_1t+s_2))\\ &= \mathrm{Tr}_{2m}(b''(s_1t)^{3^{m+j}+3^j+1} + b''(s_1t)^{3^{m+j}+1}s_2^{3^j})\\ &\quad +\mathrm{Tr}_{2m}(b''(s_1t)^{3^j+1}s_2^{3^{m+j}} + b''s_1ts_2^{3^{m+j}+3^j}\\ &\quad +b''(s_1t)^{3^m+1}s_2^{3^{-j}}) + \mathrm{Tr}_{2m}\left(b''s_1ts_2^{3^m+3^{m-j}} + b''s_1ts_2^{3^m+3^{-j}}\right.\\ &\quad \left. + b''s_2^{3^{m+j}+3^j+1}\right) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3))).\end{aligned}$$

Similarly, we have $\mathrm{Tr}_{2m}(c(s_1t+s_2)^{(3^m+1)(3^k+1)}) \in \mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. The result then follows. □

Before continuing our calculations, we introduce some convenient terminology. Let γ be a primitive element of $\mathbb{F}_{3^{2m}}$. For $0 \le k \le 2$ and $0 \le j \le 2m-1$, we define the following linear codes:

$$\begin{aligned}\mathcal{C}_{\gamma_{kj}} &= \left\{\sum_{i=0}^{3^{2m}-2}\mathrm{Tr}_{2m}(a_i\gamma_{kj}^i)x^i \mid a_i \in \mathbb{F}_{3^{2m}}\right\},\\ \mathcal{C}_{\gamma_{3j}} &= \left\{\sum_{i=0}^{3^{2m}-2}\mathrm{Tr}_{2m}(a_i\gamma_{3j}^i)x^i \mid a_i \in \mathbb{F}_{3^m}\right\},\end{aligned}$$

where $\gamma_{0j} = \gamma$, $\gamma_{1j} = \gamma^{(3^m+1)3^j+1}$, $\gamma_{2j} = \gamma^{3^j+1}$, and $\gamma_{3j} = \gamma^{(3^j+1)(3^m+1)}$. We define a linear code

$$\mathcal{C} = \left\langle x \mid x \in \mathcal{C}_{\gamma_{kj}}, 0 \le k \le 3, 0 \le j \le 2m-1\right\rangle_{\mathbb{F}_3}. \tag{4.12}$$

For $0 \le j \le 2m-1$, we set

$$\begin{aligned} S_{0j} &= \{-3^i \mid 0 \le i \le 2m-1\}, \\ S_{1j} &= \{-3^i(3^j(3^m+1)+1) \mid 0 \le i \le 2m-1\}, \\ S_{2j} &= \{-3^i(3^j+1) \mid 0 \le i \le 2m-1\}, \\ S_{3j} &= \{-3^i(3^j+1)(3^m+1) \mid 0 \le i \le 2m-1\}. \end{aligned} \tag{4.13}$$

Remark 4.11 From Theorem 3.4, $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is permutation-equivalent to the code $\overline{\mathcal{C}^{\perp}}^{\perp}$, where $\mathcal{C}$ is the linear code defined in (4.12). By Theorem 2.3, we know that each code $\mathcal{C}_{\gamma_{kj}}$, $0 \le k \le 3$, $0 \le j \le 2m-1$, has defining set $T_{kj} = \mathbb{F}_{3^{2m}}^* \setminus S_{jk}$. Then the linear code $\mathcal{C}$ has the defining set $T = \cap_{k=0}^{3} \cap_{j=0}^{2m-1} T_{kj}$ by Proposition 2.2. Let $S_k = \cup_{j=0}^{2m-1} S_{kj}$ for $0 \le k \le 3$. It is straightforward to verify that the defining set

$$T = \cap_{k=0}^{3} \cap_{j=0}^{2m-1} (\mathbb{F}_{3^{2m}}^* \setminus S_{kj}) = \cap_{k=0}^{3} (\mathbb{F}_{3^{2m}}^* \setminus (\cup_{j=0}^{2m-1} S_{kj})) = \mathbb{F}_{3^{2m}}^* \setminus (\cup_{k=0}^{3} S_k).$$

One can easily check that $S_i \cap S_j = \varnothing$ for any $0 \le i \ne j \le 3$. Now we count the number of the elements in each S_i, $0 \le i \le 3$. Note that $|S_0| = 2m$.

Lemma 4.12 *Let S_{1j}, $0 \le j \le 2m-1$, be defined in (4.13). Then we have the following:*

(1) *For any $0 \le i_1, i_2, j_1, j_2 \le 2m-1$, $-3^{i_1}(3^{j_1}(3^m+1)+1) \equiv -3^{i_2}(3^{j_2}(3^m+1)+1) \bmod (3^{2m}-1)$ if and only if $i_1 = i_2$ and $j_1 = j_2$ or $j_1 + m \equiv j_2 \bmod 2m$.*

(2) *For any $0 \le i \ne j \le 2m-1$, $|S_{1i}| = 2m$ and*

$$\begin{cases} S_{1i} = S_{1j}, & \text{if } i + m \equiv j \bmod 2m, \\ S_{1i} \cap S_{1j} = \varnothing, & \text{if } i + m \not\equiv j \bmod 2m. \end{cases}$$

(3) $|S_1| = 2m^2$.

Proof (1) Assume that $i_2 \ge i_1$. If $-3^{i_1}(3^{j_1}(3^m+1)+1) \equiv -3^{i_2}(3^{j_2}(3^m+1)+1) \bmod 3^{2m}-1$, then we have

$$3^{i_2-i_1+j_2+m} + 3^{i_2-i_1+j_2} + 3^{i_2-i_1} - 3^{j_1+m} - 3^{j_1} - 1 \equiv 0 \bmod 3^{2m}-1. \tag{4.14}$$

Let a_1, a_2, a_3 be integers such that

$$\begin{cases} 0 \le i_2 - i_1 + j_2 + m - 2a_1 m \le 2m-1, \\ 0 \le i_2 - i_1 + j_2 - 2a_2 m \le 2m-1, \\ 0 \le j_1 + m - 2a_3 m \le 2m-1. \end{cases}$$

It implies that $0 \le a_1 \le 2$, $0 \le a_2 \le 1$ and $0 \le a_3 \le 1$. We denote that

$$\begin{cases} s_1 = i_2 - i_1 + j_2 + m - 2a_1 m, \\ s_2 = i_2 - i_1 + j_2 - 2a_2 m, \\ s_3 = i_2 - i_1, \\ t_1 = j_1 + m - 2a_3 m, \\ t_2 = j_1. \end{cases}$$

Since $2 - 2 \cdot 3^{2m-1} \le 3^{s_1} + 3^{s_2} + 3^{s_3} - 3^{t_1} - 3^{t_2} - 1 \le 3^{2m} - 3$, we get that $3^{s_1} + 3^{s_2} + 3^{s_3} - 3^{t_1} - 3^{t_2} - 1 = 0$ by (4.14). Note that the set $\{s_1, s_2, s_3\}$ has at least one zero element. We have $s_2 \equiv s_1 + m \bmod 2m$, so that s_1, s_2 and s_3 are not all zero.

If there is exactly one element in $\{s_1, s_2, s_3\}$ equal to 0, then we have three cases to consider: $s_k = 0$, $\min(\{s_1, s_2, s_3\} \setminus \{s_k\}) = \min\{t_1, t_2\}$ and $\max(\{s_1, s_2, s_3\} \setminus \{s_k\}) = \max\{t_1, t_2\}$ for $1 \le k \le 3$. Therefore we get that $i_1 = i_2$ and

$$\begin{cases} j_1 = 0, j_2 = m \text{ or } j_1 = j_2 = m, & \text{if } k = 1, \\ j_1 = j_2 = 0 \text{ or } j_1 = m, j_2 = 0, & \text{if } k = 2, \\ j_1 = j_2 \text{ or } j_2 \equiv j_1 + m \bmod 2m, & \text{if } k = 3. \end{cases}$$

If there are exactly two elements in $\{s_1, s_2, s_3\}$ equal to 0, then we have $1+3^s = 3^{t_1}+3^{t_2}$, where $s \in \{s_1, s_2, s_3\}$ such that $s \neq 0$. It implies that $\min\{t_1, t_2\} = \min\{s, 0\} = 0$ and $\max\{t_1, t_2\} = \max\{s, 0\} = s$. Since $s_1 = 0$ and $s_2 = 0$ do not hold at the same time, we deduce that $s_3 = 0$, i.e. $i_1 = i_2$, and get the following four cases:

$$\begin{cases} j_1 = 0, j_2 = m, & \text{if } s_1 = 0, s_2 = t_1, t_2 = 0, \\ j_1 = j_2 = m, & \text{if } s_1 = 0, s_2 = t_2, t_1 = 0, \\ j_1 = j_2 = 0, & \text{if } s_2 = 0, s_1 = t_1, t_2 = 0, \\ j_1 = m, j_2 = 0, & \text{if } s_2 = 0, s_1 = t_2, t_1 = 0. \end{cases}$$

Summing up all these calculations, we have shown that (4.14) holds if and only if $i_1 = i_2$ and $j_1 = j_2$ or $j_1 + m \equiv j_2 \bmod 2m$.

(2) By (1), we know that $-3^{i_1}(3^j(3^m+1)+1) \equiv -3^{i_2}(3^j(3^m+1)+1) \bmod 3^{2m}-1$ if and only if $i_1 = i_2$. Therefore $|S_{1i}| = 2m$ for any $0 \le i \le 2m-1$. Let $0 \le i \neq j \le 2m-1$. Again, by (1), if $i + m \equiv j \bmod 2m$, then $S_{1i} = S_{1j}$. If $i + m \not\equiv j \bmod 2m$, then $S_{1i} \cap S_{1j} = \varnothing$.

(3) By (2), $S_1 = \cup_{i=0}^{m-1} S_{1i}$. Hence $|S_1| = \sum_{i=0}^{m-1} |S_{1i}| = 2m^2$. □

Lemma 4.13 *Let S_{2j}, $0 \le j \le 2m-1$, be defined in (4.13). Then we have the following:*

(1) *For any $0 \le i_1, i_2, j_1, j_2 \le 2m-1$, $-3^{i_1}(3^{j_1}+1) \equiv -3^{i_2}(3^{j_2}+1) \bmod (3^{2m}-1)$ if and only if $j_1 = j_2$ and $i_1 = i_2$ or $j_1 \equiv -j_2 \bmod 2m$ and $i_1 \equiv i_2 + j_2 \bmod 2m$.*

(2) *For any $0 \le i \neq j \le 2m-1$,*

$$|S_{2i}| = \begin{cases} m, & \text{if } i = m, \\ 2m, & \text{otherwise,} \end{cases}$$

and

$$\begin{cases} S_{2i} = S_{2j}, & \text{if } i \equiv -j \bmod 2m, \\ S_{2i} \cap S_{2j} = \varnothing, & \text{if } i \not\equiv -j \bmod 2m. \end{cases}$$

(3) $|S_2| = (2m+1)m$.

Proof (1) Assume that $i_2 \ge i_1$. If $3^{i_1}(3^{j_1}+1) \equiv 3^{i_2}(3^{j_2}+1) \bmod 3^{2m}-1$, then we have

$$3^{i_2-i_1+j_2} + 3^{i_2-i_1} - 3^{j_1} - 1 \equiv 0 \bmod 3^{2m}-1. \tag{4.15}$$

Let a be an integer such that $0 \le i_2 - i_1 + j_2 - 2am \le 2m-1$. Note that $0 \le a \le 1$. We denote that

$$\begin{cases} s_1 = i_2 - i_1 + j_2 - 2am, \\ s_2 = i_2 - i_1, \\ t = j_1. \end{cases}$$

Since $1-3^{2m-1} \le 3^{s_1}+3^{s_2}-3^t-1 \le 2\cdot 3^{2m-1}-2$, we have $3^{s_1}+3^{s_2}-3^t-1=0$ by (4.16). We know that at least one element of $\{s_1, s_2\}$ is equal to 0 because of $\min\{s_1, s_2\} = \min\{t, 0\} = 0$.

If there is exactly one element in $\{s_1, s_2\}$ equal to 0, then we have two cases:

$$\begin{cases} j_1 + j_2 \equiv 0 \bmod 2m, i_2 - i_1 = j_1, & \text{if } s_1 = 0, s_2 = t, \\ j_1 = j_2, i_1 = i_2, & \text{if } s_2 = 0, s_1 = t. \end{cases}$$

If $s_1 = s_2 = 0$, then $t = 0$. It induces that $j_1 = j_2 = 0$ and $i_1 = i_2$.

Then by the above discussion, we see that (4.16) holds if and only if $j_1 = j_2, i_1 = i_2$ or $j_1 + j_2 \equiv 0 \bmod 2m, i_1 \equiv i_2 + j_2 \bmod 2m$.

(2) By (1), $-3^{i_1}(3^j+1) \equiv -3^{i_2}(3^j+1) \bmod 3^{2m}-1$ if and only if

$$\begin{cases} i_1 = i_2, & \text{if } j \ne m, \\ i_1 = i_2 \text{ or } i_1 \equiv i_2 + m \bmod 2m, & \text{if } j = m. \end{cases}$$

If $j = m$, then $|S_{2j}| = m$. Otherwise, $|S_{2j}| = 2m$. Let $0 \le i \ne j \le 2m-1$. By the proof of (1), if $i + j \equiv 0 \bmod 2m$, then $S_{2i} = S_{2j}$ and if $i + j \not\equiv 0 \bmod 2m$, then $S_{2i} \cap S_{2j} = \varnothing$.

(3) By (2), we have $S_2 = \cup_{i=0}^{m} S_{2i}$. Hence $|S_2| = \sum_{i=0}^{m-1} |S_{2i}| + |S_{2,m}| = 2m^2 + m = (2m+1)m$. □

Lemma 4.14 *Let S_{3j}, $0 \le j \le 2m-1$, be defined in (4.13). Then we have the following:*

(1) For any $0 \le i_1, i_2, j_1, j_2 \le 2m-1$, $-3^{i_1}(3^{j_1}+1) \equiv -3^{i_2}(3^{j_2}+1) \bmod (3^m-1)$ if and only if $j_1 \equiv j_2 \bmod m$ and $i_1 \equiv i_2 \bmod m$ or $j_1 \equiv -j_2 \bmod m$ and $i_1 \equiv i_2 + j_2 \bmod m$.

(2) For any $0 \le i \ne j \le 2m-1$,

$$|S_{3i}| = \begin{cases} \frac{m}{2}, & \text{if } m \text{ is even and } i = \frac{m}{2} \text{ or } \frac{3m}{2}, \\ m, & \text{otherwise,} \end{cases}$$

and

$$\begin{cases} S_{3i} = S_{3j}, & \text{if } i \equiv \pm j \bmod m, \\ S_{3i} \cap S_{3j} = \varnothing, & \text{if } i \not\equiv \pm j \bmod m. \end{cases}$$

(3) $|S_3| = \frac{m(m+1)}{2}$.

Proof (1) Assume that $i_2 \ge i_1$. If $3^{i_1}(3^{j_1}+1) \equiv 3^{i_2}(3^{j_2}+1) \bmod 3^m-1$, then we have

$$3^{i_2-i_1+j_2} + 3^{i_2-i_1} - 3^{j_1} - 1 \equiv 0 \bmod 3^m - 1. \tag{4.16}$$

Let a_1, a_2, a_3 be positive integers such that

$$\begin{cases} 0 \le i_1 - i_2 + j_2 - a_1 m \le m-1, \\ 0 \le i_2 - i_1 - a_2 m \le m-1, \\ 0 \le j_1 - a_3 m \le m-1. \end{cases}$$

It implies that $0 \le a_1 \le 3$, $0 \le a_2 \le 1$ and $0 \le a_3 \le 1$. We denote that

$$\begin{cases} s_1 = i_2 - i_1 + j_2 - a_1 m, \\ s_2 = i_2 - i_1 - a_2 m, \\ t = j_1 - a_3 m. \end{cases}$$

Since $1-3^{m-1} \le 3^{s_1}+3^{s_2}-3^t-1 \le 2\cdot 3^{m-1}-2$, we get $3^{s_1}+3^{s_2}-3^t-1=0$ by (4.16). The set $\{s_1, s_2\}$ contains at least one zero element because of $\min\{s_1, s_2\} = \min\{t, 0\} = 0$.

If there is exactly one element in $\{s_1, s_2\}$ equal to 0, then we get two cases:

$$\begin{cases} j_1 \equiv -j_2 \bmod m, i_1 \equiv i_2 + j_2 \bmod m, & \text{if } s_1 = 0, s_2 = t, \\ j_1 \equiv j_2 \bmod m, i_1 \equiv i_2 \bmod m, & \text{if } s_2 = 0, s_1 = t. \end{cases}$$

If $s_1 = s_2 = 0$, then $t = 0$. It induces that $j_1 \equiv j_2 \equiv 0 \bmod m$ and $i_1 \equiv i_2 \bmod m$.

From the above discussion, we conclude that (4.16) holds if and only if $j_1 \equiv j_2 \bmod m$, $i_1 \equiv i_2 \bmod m$ or $j_1 \equiv -j_2 \bmod m$, $i_1 \equiv i_2 + j_2 \bmod m$.

(2) By (1), we see that $-3^{i_1}(3^j+1) \equiv -3^{i_2}(3^j+1) \bmod 3^m-1$ if and only if

$$\begin{cases} i_1 \equiv i_2 \bmod m \text{ or } i_1 \equiv i_2 + \frac{m}{2} \bmod m, & \text{if } m \text{ is even and } j = \frac{m}{2} \text{ or } \frac{3m}{2}, \\ i_1 \equiv i_2 \bmod m, & \text{otherwise.} \end{cases}$$

Therefore, if m is even, $|S_{3,\frac{m}{2}}| = |S_{3,\frac{3m}{2}}| = \frac{m}{2}$ and $|S_{3i}| = m$ for any $0 \le i \le 2m-1$ and $i \ne \frac{m}{2}, \frac{3m}{2}$. If m is odd, $|S_{3i}| = m$ for any $0 \le i \le 2m-1$. We also get that $S_{3i} = S_{3j}$, if $i \equiv \pm j \bmod m$ and $S_{3i} \cap S_{3j} = \varnothing$, if $i \not\equiv \pm j \bmod m$.

(3) By (2), if m is even, then $|S_3| = \sum_{i=0}^{\frac{m}{2}-1} |S_{3i}| + |S_{3,\frac{m}{2}}| = \frac{m^2}{2} + \frac{m}{2} = \frac{m(m+1)}{2}$. If m is odd, then $|S_3| = \sum_{i=0}^{\frac{m-1}{2}} |S_{3i}| = \frac{m(m+1)}{2}$. Hence $|S_3| = \frac{m(m+1)}{2}$ for any integer $m \ge 2$. □

Proof of Theorem 3.5 By Lemma 4.12, Lemma 4.13 and Lemma 4.14, $|S| = \sum_{i=0}^{3} |S_i| = 2m + 2m^2 + (2m+1)m + \frac{m(m+1)}{2} = \frac{9m^2+7m}{2}$. Now we have $\dim(\mathcal{C}) = n - |T| = n - (n - |S|) = \frac{9m^2+7m}{2}$. Then

$$\dim(\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))) = \dim(\overline{\mathcal{C}^{\perp}}^{\perp}) = \dim(\mathcal{C}) + 1 = \frac{9m^2+7m}{2} + 1.$$

The linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is a subcode of the 4-th order generalized Reed-Muller code $\mathcal{R}_3(4,2m)$ and $\mathcal{R}_3(4,2m)$ has minimum distance 3^{2m-2} by Theorem 3.3 and Theorem 2.7. It follows that the minimum distance of $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is lower bounded by 3^{2m-2}. □

Remark 4.15 From Theorem 2.7, the 4-th order generalized Reed-Muller code $\mathcal{R}_3(4,2m)$ has dimension

$$\begin{aligned} k &= \binom{2m+3}{4} + \binom{2m+2}{3} - \frac{(2m-1)2m}{2} + 1 \\ &> \frac{9m^2+7m}{2} + 1 \\ &= \dim(\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))). \end{aligned}$$

5 Concluding remarks

In this paper, we computed the incidence matrix of the 2-design supported by the minimum weight codewords of $\mathcal{C}(2m,3)$. The linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ with $m \ge 2$ generated by the rows of the incidence matrix contains $\mathcal{C}(2m,3)$ as a subcode and has many affine invariant subcodes. This implies that the structure of the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ we obtained is richer than the original code $\mathcal{C}(2m,3)$. We proved that the linear code

$\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ is a subcode of the 4-th order generalized Reed-Muller code and developed the lower bound on the minimum weight of $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$. The dimension of the linear code $\mathcal{C}_3(\mathbb{D}_d(\mathcal{C}(2m,3)))$ was settled by counting the number of elements in the defining set of the code $\mathcal{C}$ defined in (4.12).

Acknowledgments The work of the first author was supported by The National Natural Science Foundation of China under Grant No. 11771392.

Funding National Natural Science Foundation of China under Grant No. 11771392.

References

1. Assmus Jr., E.F., Key, J.D.: Polynomial codes and finite geometries. In: Pless, V.S., Huffman, W.C. (eds.) The Handbook of Coding Theory, vol. II, pp. 1269–1343. Elsevier, Amsterdam (1998)
2. Assmus Jr., E.F., Key, J.D.: Designs and their Codes. Cambridge University Press, Cambridge (1992)
3. Ding, C.: Designs from Linear Codes. World Scientific, Singapore (2018)
4. Ding, C., Tang, C., Tonchev, D.: Linear codes of 2-designs associated with subcodes of the ternary generalized Reed-Muller codes. Des. Codes Cryptogr. **88**, 625–641 (2020)
5. Ding, C., Tang, C.: Infinite families of near MDS codes holding t-designs. IEEE Trans. Inf. Theory **66**(9), 5419–5428 (2020)
6. Ding, C.: Infinite families of 3-designs from a type of five-weight code. Des. Codes Cryptogr. **86**(3), 703–719 (2018)
7. Ding, C., Li, C.: Infinite families of 2-designs and 3-designs from linear codes. Discrete Math. **340**(10), 2415–2431 (2017)
8. Du, X., Wang, R., Tang, C., Wang, Q.: Infinite families of 2-designs from two classes of binary cyclic codes with three nonzeros. Adv. Math. Commun., https://doi.org/10.3934/amc.2020106 (2020)
9. 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] (2019)
10. Huffman, W.C., Pless, V.: Fundamentals of Error Correcting Codes. Cambridge University Press, Cambridge (2003)
11. Tang, C., Ding, C.: An infinite family of linear codes supporting 4-designs. IEEE Trans. Inf. Theory, https://doi.org/10.1109/TIT.2020.3032600 (2020)
12. Wang, R., Du, X., Fan, C.: Infinite families of 2-designs from a class of non-binary Kasami cyclic codes. Adv. Math. Commun., https://doi.org/10.3934/amc.2020088 (2019)
13. Wan, Z.: Finite Fields and Galois Rings. World Scientific, USA (2011)