J. Korean Math. Soc. **58** (2021), No. 1, pp. 29–44
https://doi.org/10.4134/JKMS.j190429
pISSN: 0304-9914 / eISSN: 2234-3008

CONSTRUCTION OF TWO- OR THREE-WEIGHT BINARY LINEAR CODES FROM VASIL'EV CODES

Jong Yoon Hyun and Jaeseon Kim

Abstract. The set D of column vectors of a generator matrix of a linear code is called a defining set of the linear code. In this paper we consider the problem of constructing few-weight (mainly two- or three-weight) linear codes from defining sets. It can be easily seen that we obtain an one-weight code when we take a defining set to be the nonzero codewords of a linear code. Therefore we have to choose a defining set from a non-linear code to obtain two- or three-weight codes, and we face the problem that the constructed code contains many weights. To overcome this difficulty, we employ the linear codes of the following form:

Let D be a subset of $\mathbb{F}_2^n$, and W (resp. V) be a subspace of $\mathbb{F}_2$ (resp. $\mathbb{F}_2^m$). We define the linear code $\mathcal{C}_D(W;V)$ with defining set D and restricted to W, V by

$$\mathcal{C}_D(W;V) = \{(s + u \cdot x)_{x \in D^*} \mid s \in W, u \in V\}.$$

We obtain two- or three-weight codes by taking D to be a Vasil'ev code of length $n = 2^m - 1 (m \geq 3)$ and a suitable choices of W. We do the same job for D being the complement of a Vasil'ev code.

The constructed few-weight codes share some nice properties. Some of them are optimal in the sense that they attain either the Griesmer bound or the Grey-Rankin bound. Most of them are minimal codes which, in turn, have an application in secret sharing schemes. Finally we obtain an infinite family of minimal codes for which the sufficient condition of Ashikhmin and Barg does not hold.

1. Introduction

Let q be a prime power and $D = \{y_1, y_2, \ldots, y_n\}$ a subset of $\mathrm{GF}(q)^k \setminus \{\mathbf{0}\}$. Calderbank and Kantor([2]) considered the code $\mathcal{C}_D$ defined by

$$\mathcal{C}_D = \{(u \cdot y_1, \ldots, u \cdot y_n) : u \in \mathrm{GF}(q)^k\} \tag{1}$$

Received June 20, 2019; Revised June 2, 2020; Accepted September 21, 2020.
2010 *Mathematics Subject Classification.* 94B05.
Key words and phrases. Vasil'ev code, Grey-Rankin bound, minimal linear codes, few-weight codes.
The first author was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(MEST) (2014R1A1A2A10054745).

and observed that every linear code can be arisen in this way. Indeed, for a given linear code $\mathcal{C}$, it can be written as $\mathcal{C}_D$, where D is the set of column vectors of a generator matrix of $\mathcal{C}$. If $\mathcal{C} = \mathcal{C}_D$, it is called that $\mathcal{C}$ is the linear code with a defining set D and D is called a defining set of $\mathcal{C}$.

In this paper we restrict ourselves to the binary case and consider the problem of constructing few-weight (mainly two- or three-weight) linear codes from a 'good' choice of defining set D. It is natural we first consider the simplest case, namely when D consists of nonzero codewords of a linear code. In this case, one can show that $\mathcal{C}_D$ is a one-weight code, in fact, if D is the nonzero codewords of a linear code of dimension k, the weight of $c(u) \triangleq (u \cdot y_1, \ldots, u \cdot y_n)$ becomes 0 when u belongs to $D^\perp$, the dual code of D, while the weight becomes 2^{k-1} when u does not belong to $D^\perp$. Therefore we have to choose D from a non-linear code to obtain two- or three-weight codes, and in turn we face the problem that $\mathcal{C}_D$ contains many weights. To overcome this difficulty, we modify the construction of Calderbank and Kantor and consider the codes of the following form:

Let D be a subset of $\mathbb{F}_2^n$, and W (resp. V) be a subspace of $\mathbb{F}_2$ (resp. $\mathbb{F}_2^n$). We define the linear code $\mathcal{C}_D(W; V)$ with defining set D and restricted to W, V by

$$\mathcal{C}_D(W; V) = \{(s + u \cdot x)_{x \in D^*} \mid s \in W, u \in V\}.$$

The codeword $(s + u \cdot x)_{x \in D^*}$ of $\mathcal{C}_D(W; V)$ will be denoted by $c(s, u)$ in the sequel. It is obvious that the code $\mathcal{C}_D(0; \mathbb{F}_2^n)$ is the same as Calderbank and Kantor's code $\mathcal{C}_D$ and that $\mathcal{C}_D(0; V)$ is a subspace of $\mathcal{C}_D(0; \mathbb{F}_2^n)$. We will obtain two- or three-weight codes by a suitable choices of W. Since $c(0, u)$ and $c(1, u)$ are complement of each other, $\mathcal{C}_D(\mathbb{F}_2; V)$ is a self-complementary code. Therefore our code $\mathcal{C}_D(\mathbb{F}_2; \mathbb{F}_2^n)$ may be considered as the 'self-complementation' of Calderbank and Kantor's code $\mathcal{C}_D$. We will see later that $\mathcal{C}_D(0; V)$ is optimal in the sense that they meet the Grey-Rankin bound for a suitable choice of V.

In this paper, we investigate the linear code $\mathcal{C}_D(\mathbb{F}_2; \mathbb{F}_2^n)$ where D is a Vasil'ev code of length $2^{m+1} - 1$ with $m \geq 2$. We determine its weight distribution and we find out several classes of two- or three-weight linear codes which are contained in $\mathcal{C}_D(\mathbb{F}_2; \mathbb{F}_2^n)$. We also do the same work for $\mathcal{C}_{D^c}(\mathbb{F}_2; \mathbb{F}_2^n)$, where D^c is the complement of the Vasil'ev code D. The two- or three-weight linear codes constructed in this way have some nice properties. Some of them are optimal in the sense that they attain either the Griesmer bound or the Grey-Rankin bound. Most of them are minimal codes which, in turn, have an application in secret sharing schemes. Finally we obtain an infinite family of minimal codes for which the sufficient condition of Ashikhmin and Barg does not hold. This is an interesting result in the sense that the construction of an infinite family of binary minimal linear codes which does not satisfy AB-condition is a hard problem in general as mentioned in [6].

The paper is organized as follows:

In Section 2, we briefly introduce basic notion of coding theory which will be necessary in our subsequent developments. In Section 3, we determine the weight distributions of $\mathcal{C}_D(\mathbb{F}_2;\mathbb{F}_2^n)$, where D is a Vasil'ev code or its complement. In Section 4, we find out several classes of subcodes in $\mathcal{C}_D(\mathbb{F}_2;\mathbb{F}_2^n)$ which are two- or three-weight codes.

2. Preliminaries

In this section, we briefly introduce basic notion of coding theory, Vasil'ev codes and defining sets which will be necessary in our subsequent developments.

Let $\mathbb{F}_2$ be the finite field with two elements, say 0 and 1, and $\mathbb{F}_2^n$ the vector space of n-tuples of elements in $\mathbb{F}_2$. We denote by $\mathbb{E}_2^n$ the subspace of even weight vectors in $\mathbb{F}_2^n$.

The support of a vector u in $\mathbb{F}_2^n$ is the set of non-zero coordinate positions of u. An $[n,k,d]$ code is a k-dimensional subspace of $\mathbb{F}_2^n$ with minimum (Hamming) distance d. A linear code is called self-complementary if it contains the complement $\bar{u}$ of any codeword u.

The Griesmer bound [9] states that if C is a $[n,k,d]$ linear code, then

$$n \geq \sum_{i=0}^{k-1} \left\lceil \frac{d}{2^i} \right\rceil,$$

and the Grey-Rankin bound [10] states that

$$2^k \leq \frac{8d(n-d)}{n-(n-2d)^2} \tag{2}$$

for any $[n,k,d]$ self-complementary linear code provided that the right-hand side is positive.

Let C be a linear code of length n, and A_i the number of codewords of C of weight i. The sequence $(A_0, A_1, \ldots, A_n)$ is called the weight distribution of C and it is denoted by $wd(C)$. By linearity, we always have $A_0 = 1$. A code C is called a t-weight code if there are t non-zero weights, i.e., the number of non-zero indices i such that $A_i > 0$ is equal to t. The weight enumerator of a linear code of length n is defined by $1 + A_1 z + A_2 z^2 + \cdots + A_n z^n$.

In 1962, Vasil'ev constructed a family of binary nonlinear 1-error correcting perfect codes as follows: Let $\mathcal{C}$ be a perfect code (not necessarily linear) of length $2^m - 1$ and $\lambda : \mathcal{C} \to \mathbb{F}_2$ be any mapping with $\lambda(\mathbf{0}) = 0$. Set $\pi(u) = 0$ or 1 depending on whether $wt(u)$ is even or odd. Then one can check that the code defined by

$$\mathcal{V} = \{(u|u+v|\pi(u)+\lambda(v)) \,|\, u \in \mathbb{F}_2^{2^m-1}, v \in \mathcal{C}\}$$

becomes a perfect code of length $2^{m+1} - 1$. It is also known that $\mathcal{V}$ is not a linear code if λ is not linear, i.e., $\lambda(v+v') \neq \lambda(v)+\lambda(v')$ for some elements v, v' of $\mathcal{C}$. The codes $\mathcal{V}$ constructed in this way are called Vasil'ev codes associated with $\mathcal{C}$. In this paper, we fix $\mathcal{C}$ to be the Hamming code H_m of length $2^m - 1$ and we utilize several Vasil'ev codes by varying nonlinear function λ.

Let D be a subset of $\mathbb{F}_2^n$ and $D^* = D \setminus \{\mathbf{0}\}$, where $\mathbf{0}$ is the zero-vector. The rank of D, denoted by $\mathrm{rank}(D)$, is the dimension of its linear span $\langle D \rangle$. The dual $D^\perp$ of D is defined by

$$\{u \in \mathbb{F}_2^n : u \cdot v = 0 \text{ for all } v \in D\},$$

where the inner product is the usual one. It is easily seen that $D^\perp$ is a subspace of $\mathbb{F}_2^n$ and $\dim(D^\perp) = n - \mathrm{rank}(D)$. The indicator function $\mathbb{1}_D$ is a function of $\mathbb{F}_2^n$ to $\mathbb{F}_2$ which is defined by $\mathbb{1}_D(u) = 1$ if and only if $u \in D$. We define

$$\mathcal{C}_D(W;V) = \{c_D(s,u) = (s + u \cdot x)_{x \in D^*} : s \in V, u \in W\},$$

where W is a subspace of $\mathbb{F}_2$ and V is a subspace of $\mathbb{F}_2^n$. Then $\mathcal{C}_D(W;V)$ is a linear code of length $|D^*|$ and its dimension is at most $\dim(W) + \dim(V)$. We notice that $\mathcal{C}_D(W;V)$ is a self-complementary code when $W = \mathbb{F}_2$. The weight of a codeword $c_D(s,u)$ in $\mathcal{C}_D(W;V)$ is given by

$$\mathrm{wt}(c_D(s,u)) = |D^*| - \frac{1}{2}\sum_{y \in \mathbb{F}_2}\sum_{x \in D^*}(-1)^{y(s+u\cdot x)} = \frac{1}{2}|D^*| - \frac{1}{2}(-1)^s \chi_u(D^*), \tag{3}$$

where $\chi_u(D^*) = \sum_{x \in D^*}(-1)^{u\cdot x}$. We also compute the weight $c_{D^c}(s,u)$ of a codeword in $\mathcal{C}_{D^c}(W;V)$, where D^c is the complement of D in $\mathbb{F}_2^n$. The relation

$$\sum_{x \in D^c}(-1)^{u\cdot x} = \sum_{x \in \mathbb{F}_2^n}(-1)^{u\cdot x} - \sum_{x \in D}(-1)^{u\cdot x},$$

together with (3) lead to

$$\mathrm{wt}(c_{D^c}(s,u)) = \frac{1}{2}(|D^c| - (-1)^s 2^n \delta_{u,0}) + \frac{(-1)^s}{2}\chi_u(D), \tag{4}$$

where δ is the Kronecker delta function.

A codeword c *covers* a codeword c' if the support of c contains that of c'. A codeword c is *minimal* if it covers only its multiples. A linear code is called *minimal* if every non-zero codeword is minimal. Minimal linear codes have an important application [7] in building secret sharing schemes which are cryptographic primitive that enables us to distribute a secret among multiple users. Secret sharing schemes constructed by minimal linear codes are known to have minimal assess sets. Of particular interest is that in a secret sharing scheme designed by a linear code C, to determine minimal access sets is equivalent to find the minimal codewords of the dual code $C^\perp$.

Ashikhmin and Barg [1] gave a sufficient condition for a linear code to be minimal: A q-ary linear code C with minimum distance d is minimal provided that $\frac{d}{d_{\max}} > \frac{q-1}{q}$, where $d_{\max}$ is the maximum weight of C. We refer to this condition as AB-condition. Ding, Heng and Zhou [6] gave a sufficient and necessary condition for a binary linear code to be minimal: A binary linear code is minimal if and only if for each pair of distinct nonzero codewords a and b,

$$\mathrm{wt}(a+b) \neq \mathrm{wt}(a) - \mathrm{wt}(b).$$

This condition gives another sufficient condition for a linear code to be minimal: If C is a two-weight linear code of length n and weights w_1 and w_2 where $0 < w_1 < w_2 < n$ with $w_2 \neq 2w_1$, then it is minimal. We refer to this condition as DHZ-condition.

We refer to [1, 5, 7] for further information on minimal linear codes.

3. Construction of linear codes from Vasil'ev codes

In this section, we construct several classes of linear codes from Vasil'ev codes which are used in the next section.

Let H_m ($m \geq 2$) be the Hamming code with parameters $[n = 2^m - 1, n - m, 3]$ and λ a nonlinear function from H_m to $\mathbb{F}_2$ with $\lambda(\mathbf{0}) = 0$. Set $\pi(u) = wt(u) \pmod 2$. We consider the Vasil'ev code ([11])

$$D_m^\lambda = \{(u|u+v|\pi(u) + \lambda(v)) : u \in \mathbb{F}_2^n, v \in H_m\},$$

which is not linear. We simply denote it by D. It is known [9] that D is a perfect binary code of length $2n+1 = 2^{m+1}-1$, size 2^{2n-m}, minimum distance 3. Furthermore, Etzion and Vardy [8] verified

$$\operatorname{rank}(D) = \operatorname{rank}(H_m) + n + 1 = 2n - m + 1. \tag{5}$$

Let $u = (u_1|u_2|t)$ be a codeword in D. We first compute the weight of $c_D(s, u)$ in $\mathcal{C}_D$. It follows from the definition that

$$\begin{aligned}
\chi_u(D) &= \sum_{x_1 \in \mathbb{F}_2^n, x_2 \in H_m} (-1)^{u_1 \cdot x_1 + u_2 \cdot (x_1 + x_2) + t(\pi(x_1) + \lambda(x_2))} \\
&= \sum_{x_2 \in H_m} \sum_{x_1 \in \mathbb{F}_2^n} (-1)^{(u_1+u_2)\cdot x_1 + t\pi(x_1)} (-1)^{u_2 \cdot x_2 + t\lambda(x_2)} \\
&= \Big(\sum_{x_2 \in H_m} (-1)^{u_2 \cdot x_2 + t\lambda(x_2)} \Big) \Big(\sum_{x_1 \in \mathbb{F}_2^n} (-1)^{(u_1+u_2)\cdot x_1 + t\pi(x_1)} \Big) = \alpha\beta,
\end{aligned}$$

where $\alpha = \sum_{x_2 \in H_m} (-1)^{u_2 \cdot x_2 + t\lambda(x_2)}$ and $\beta = \sum_{x_1 \in \mathbb{F}_2^n} (-1)^{(u_1+u_2)\cdot x_1 + t\pi(x_1)}$. It follows from $(-1)^v = 1 - 2v$ for $v \in \mathbb{F}_2$ that

$$\begin{aligned}
\alpha &= \sum_{x_2 \in H_m} (1 - 2t\lambda(x_2))(-1)^{u_2 \cdot x_2} \\
&= \sum_{x_2 \in H_m} (-1)^{u_2 \cdot x_2} - 2t \sum_{x_2 \in H_m} \lambda(x_2)(-1)^{u_2 \cdot x_2} \\
&= 2^{n-m} \mathbb{1}_{H_m^\perp}(u_2) - 2t \sum_{x_2 \in \lambda^{-1}(1)} (-1)^{u_2 \cdot x_2},
\end{aligned}$$

and if $\mathbb{E}_2^n$ is the subspace consisting of all even weight vectors in $\mathbb{F}_2^n$, then

$$\beta = \sum_{x_1 \in \mathbb{F}_2^n} (-1)^{t\pi(x_1)} (-1)^{(u_1+u_2)\cdot x_1}$$

$$
\begin{aligned}
&= \sum_{x_1 \in \mathbb{E}_2^n} (-1)^{(u_1+u_2)\cdot x_1} + (-1)^t \sum_{x_1 \in \mathbb{F}_2^n \setminus \mathbb{E}_2^n} (-1)^{(u_1+u_2)\cdot x_1} \\
&= 2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2) + (-1)^t \Big(\sum_{x_1 \in \mathbb{F}_2^n} (-1)^{(u_1+u_2)\cdot x_1} + \sum_{\mathbb{E}_2^n} (-1)^{(u_1+u_2)\cdot x_1} \Big) \\
&= 2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2) + (-1)^t \left(2^n \delta_{u_1,u_2} - 2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2)\right),
\end{aligned}
$$

because the dual of $\mathbb{E}_2^n$ equals $\langle \mathbf{1} \rangle$ generated by the all-ones vector $\mathbf{1}$. It then follows from (3) and

$$\chi_u(D) = \chi_u(D^*) + 1$$

that $\mathrm{wt}(c_D(s,u))$ becomes

$$
\begin{aligned}
(6) \qquad & \frac{1}{2}(|D^*| + (-1)^s) - \frac{(-1)^s}{2}\Big(2^{n-m}\mathbb{1}_{H_m^\perp}(u_2) - 2t\chi_{u_2}(\lambda^{-1}(1))\Big) \\
& \times \Big(2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2) + (-1)^t(2^n\delta_{u_1,u_2} - 2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2))\Big)
\end{aligned}
$$

and it follows from (4) that $\mathrm{wt}(c_{D^c}(s,u))$ becomes

$$
\begin{aligned}
(7) \qquad & \frac{1}{2}(|D^c| - (-1)^s 2^{2n+1}\delta_{u,0}) + \frac{(-1)^s}{2}\Big(2^{n-m}\mathbb{1}_{H_m^\perp}(u_2) - 2t\chi_{u_2}(\lambda^{-1}(1))\Big) \\
& \times \Big(2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2) + (-1)^t(2^n\delta_{u_1,u_2} - 2^{n-1}\mathbb{1}_{\langle \mathbf{1} \rangle}(u_1+u_2))\Big).
\end{aligned}
$$

We are going to compute the weights in (6) and (7) explicitly for a suitable choice of the nonlinear function λ.

Case 1: $\boldsymbol{\lambda^{-1}(1)}$ is a linear subcode in $\boldsymbol{H_m}$

We first consider the case $\lambda^{-1}(1) = C^*$ where C is a linear subcode in H_m of dimension $k \geq 1$. If $k = 1$, then there are $x_1 \in C^*$ and $x_2 \in H_m \setminus C$ such that $x_1 + x_2 \in H_m \setminus C$ and if $k \geq 2$, then there are y_1 and y_2 in C^* such that $y_1 + y_2 \in C^*$, so that λ is nonlinear in any case. We obtain that

$$
(8) \qquad \chi_{u_2}(\lambda^{-1}(1)) = \sum_{x_2 \in \lambda^{-1}(1)} (-1)^{u_2 \cdot x_2} = 2^k \mathbb{1}_{C^\perp}(u_2) - 1.
$$

It follows from (6) and (8) that the weight of $c_D(s,u) = c(s,(u_1|u_2|t))$ is equal to

(9)
$$wt(c_D(s,u)) = \begin{cases} 0 & \text{if } s=0, u_1=u_2 \in H_m^\perp, t=0, \\ 2^{n+k}-2^n & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=1, \\ 2^{2n-m-1}-2^{n+k}+2^n-1 & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n-m-1}-2^n & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \\ 2^{2n-m-1}-1 & \text{if } \begin{cases} s=1, u_1 \neq u_2 \text{ or } u_2 \notin H_m^\perp, t=1, \\ s=1, u_1+u_2 \neq \mathbf{1}, t=1, \end{cases} \\ 2^{2n-m-1} & \text{if } \begin{cases} s=0, u_1 \neq u_2 \text{ or } u_2 \notin H_m^\perp, t=0, \\ s=0, u_1+u_2 \neq \mathbf{1}, t=1, \end{cases} \\ 2^{2n-m-1}+2^n-1 & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \\ 2^{2n-m-1}+2^{n+k}-2^n & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n-m}-2^{n+k}+2^n-1 & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=1, \\ 2^{2n-m}-1 & \text{if } s=1, u_1=u_2 \in H_m^\perp, t=0, \end{cases}$$

and from (7) and (8) that the weight of $c_{D^c}(s,u) = c(s,(u_1|u_2|t))$ is equal to

(10)
$$wt(c_{D^c}(s,u)) = \begin{cases} 0 & \text{if } s=0, u_1=u_2=0, t=0, \\ 2^{2n}-2^{2n-m} & \text{if } s=1, u_1=u_2 \in H_m^\perp \setminus \{0\}, t=0, \\ 2^{2n}-2^{2n-m}+2^{n+k}-2^n & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=0, \\ 2^{2n}-2^{2n-m-1}-2^{n+k}+2^n & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n}-2^{2n-m-1}-2^n & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \\ 2^{2n}-2^{2n-m-1} & \text{if } \begin{cases} u_1 \neq u_2 \text{ or } u_2 \notin H_m^\perp, t=0, \\ u_1+u_2 \neq \mathbf{1}, t=1, \end{cases} \\ 2^{2n}-2^{2n-m-1}+2^n & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \\ 2^{2n}-2^{2n-m-1}+2^{n+k}-2^n & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n}-2^{n+k}+2^n & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=0, \\ 2^{2n} & \text{if } s=0, u_1=u_2 \in H_m^\perp \setminus \{0\}, t=0, \\ 2^{2n+1}-2^{2n-m} & \text{if } s=1, u_1=u_2=0, t=0. \end{cases}$$

Case 2: $\boldsymbol{\lambda^{-1}(1)}$ is the complement of a linear subcode in $\boldsymbol{H_m}$

We next consider the case $\lambda^{-1}(1) = H_m \setminus C$, where C is a linear subcode in H_m of dimension $1 \leq k \leq n-m-2$. Then there are $x_1, x_2 \in H_m \setminus C$ such that $x_1 + x_2 \in H_m \setminus C$, so that λ is nonlinear. We obtain that

$$\chi_{u_2}(\lambda^{-1}(1)) = \sum_{x_2 \in \lambda^{-1}(1)} (-1)^{u_2 \cdot x_2} = 2^{n-m} \mathbb{1}_{H_m^\perp}(u_2) - 2^k \mathbb{1}_{C^\perp}(u_2). \tag{11}$$

Using (6) and (11), the weight of $c_D(s,u) = c(s,(u_1|u_2|t))$ is equal to

$$(12)\quad wt(c_D(s,u)) = \begin{cases} 0 & \text{if } s=0, u_1=u_2 \in H_m^\perp, t=0, \\ 2^{n+k}-1 & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=1, \\ 2^{2n-m-1}-2^{n+k} & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n-m-1}-1 & \text{if } \begin{cases} s=1, u_1 \neq u_2 \text{ or } u_2 \notin H_m^\perp, t=0, \\ s=1, u_1+u_2 \neq \mathbf{1}, t=1, \\ s=1, u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \end{cases} \\ 2^{2n-m-1} & \text{if } \begin{cases} s=0, u_1 \neq u_2 \text{ or } u_2 \notin H_m^\perp, t=0, \\ s=0, u_1+u_2 \neq \mathbf{1}, t=1, \\ s=0, u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \end{cases} \\ 2^{2n-m-1}+2^{n+k}-1 & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n-m}-2^{n+k} & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=1, \\ 2^{2n-m}-1 & \text{if } s=1, u_1=u_2 \in H_m^\perp, t=0, \end{cases}$$

and using (7) and (11), the weight of $c_{D^c}(s,u) = c(s,(u_1|u_2|t))$ is equal to

(13)

$$wt(c_{D^c}(s,u)) = \begin{cases} 0 & \text{if } s=0, u_1=u_2=0, t=0, \\ 2^{2n}-2^{2n-m} & \text{if } s=1, u_1=u_2 \in H_m^\perp \setminus \{0\}, t=0, \\ 2^{2n}-2^{2n-m}+2^{n+k} & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=1, \\ 2^{2n}-2^{2n-m-1}-2^{n+k} & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n}-2^{2n-m-1} & \text{if } \begin{cases} u_1 \neq u_2 \text{ or } u_2 \notin H_m^\perp, t=0, \\ u_1+u_2 \neq \mathbf{1}, t=1, \\ u_1+u_2=\mathbf{1}, u_2 \notin C^\perp, t=1, \end{cases} \\ 2^{2n}-2^{2n-m-1}+2^{n+k} & \text{if } s=0, u_1+u_2=\mathbf{1}, u_2 \in C^\perp \setminus H_m^\perp, t=1, \\ 2^{2n}-2^{n+k} & \text{if } s=1, u_1+u_2=\mathbf{1}, u_2 \in H_m^\perp, t=1, \\ 2^{2n} & \text{if } s=0, u_1=u_2 \in H_m^\perp \setminus \{0\}, t=0. \\ 2^{2n+1}-2^{2n-m} & \text{if } s=1, u_1=u_2=0, t=0. \end{cases}$$

Our next job is to compute the frequency for each weight. We need the following lemma.

Lemma 3.1. *Let H_m be the Hamming code of length $n=2^m-1$ for $m \geq 2$ and D a Vasil'ev code associated with the Hamming code H_m. Let W be a subspace of $\mathbb{F}_2$ and V a subspace of $\mathbb{F}_2^{2n+1}$. Then the following statements are true.*

(i) *If V contains $\{(v|v|0)|v \in H_m^\perp\}$, then* $\dim(\mathcal{C}_D(W;V)) = \dim(W) + \dim(V) - m$,

(ii) $\dim(\mathcal{C}_{D^c}(W;V)) = \dim(W) + \dim(V)$.

Proof. (i) Let's consider the map $\phi : W \times V \to \mathcal{C}_D(W;V)$ by $(s,u) \mapsto c_D(s,u)$. Then ϕ is a surjective homomorphism by the definition of $\mathcal{C}_D(W;V)$. First of all, we claim that the kernel of ϕ is the set $\{0\} \times D^\perp$. Let $(s,u) \in \mathbb{F}_2 \times \mathbb{F}_2^n$ be in the kernel of ϕ. This implies that

$$(14)\qquad s + u \cdot x = 0 \text{ for all } x \in D^*.$$

Let v and w be distinct vectors in $\mathbb{F}_2^{n*}$. For two distinct vectors $x' = (v|v|\pi(v))$, $x'' = (w|w|\pi(w))$ in D^*, we have that $x' + x''$ is also in D^* because π is linear. These two vectors give that

$$s = u \cdot (x' + x'') = u \cdot x' + u \cdot x'' = s + s = 0, \tag{15}$$

so (s, u) is in $\{0\} \times (D^\perp \cap V) = \{0\} \times D^\perp$ since $D^\perp \subseteq V$ by our assumption. The opposite inclusion is obvious. Note that $\{(v|v|0)|v \in H_m^\perp\}] \subseteq D^\perp$ and the rank of D is to be $2n + 1 - m$ by (5), we conclude that $D^\perp = \{(v|v|0)|v \in H_m^\perp\}$. It is follows from $\mathcal{C}_D(W; V)$ is isomorphic to $(W \times V)/(\text{kernel of } \phi)$ that we have $\dim(\mathcal{C}_D(W; V)) = \dim(W) + \dim(V) - \dim(H_m^\perp)$ and the proof is completed.

(ii) We define $\varphi : W \times V \to \mathcal{C}_{D^c}(W; V)$ by $(s, u) \mapsto c_{D^c}(s, u)$. As in (i), we see that the kernel of φ is the set $\{0\} \times (D^c)^\perp$. Note that any vector whose weight is one is in D^c because the minimum distance of D is three. Hence the rank of D^c should be $2n + 1$, so that $(D^c)^\perp = \{\mathbf{0}\}$ and the proof is completed. □

The following Lemmas 3.2 and 3.3 will play an important role in deriving Proposition 4.1 and Theorems 4.3 and 4.5 which are main results of this paper.

Lemma 3.2. *Let H_m be the Hamming code of length $n = 2^m - 1$ for $m \geq 2$ and D a Vasil'ev code corresponding to a nonlinear function λ on H_m. Let C be a linear subcode of H_m. Let $W = \mathbb{F}_2$ and $V = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$.*

(1) *Set $\lambda^{-1}(1) = C^*$, where $\dim C = k$.*
   (i) *If $1 \leq k \leq n - m - 2$, then $\mathcal{C}_D(W; V)$ is a nine-weight linear code with parameters $[2^{2n-m} - 1, 2n - m + 2, 2^{n+k} - 2^n]$ whose weight distribution is given by Table 1.*
   (ii) *If k is either $n-m-1$ or $n-m$, then $\mathcal{C}_D(W; V)$ is a seven-weight linear code with parameters $[2^{2n-m} - 1, 2n - m + 2, 2^n - 1]$ whose weight distribution is given by Table 2.*

(2) *Set $\lambda^{-1}(1) = H_m \setminus C$, where $\dim C = k$.*
   If $1 \leq k \leq n - m - 2$, then $\mathcal{C}_D(W; V)$ is a seven-weight linear code with parameters $[2^{2n-m} - 1, 2n - m + 2, 2^{n+k} - 1]$ whose weight distribution is given by Table 3.

Proof. Since $W = \mathbb{F}_2$ and $V = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$, the dimension of $\mathcal{C}_D(W; V)$ is $2n - m + 2$ by Lemma 3.1(1). The non-zero weights of the code are given by (9).

To find the frequency for each non-zero weight, we need to count the number of vectors satisfying the condition for each weight. For example, consider the case $u_1 + u_2 = \mathbf{1}$ and $u_2 \in C^\perp \setminus H_m^\perp$ in 9 where C is a subspace of H_m of dimension k. Let $S = C^\perp \setminus H_m^\perp$. The number of vectors $(u_1, u_2) \in \mathbb{F}_2^n \times S$ such that $u_1 + u_2 = \mathbf{1}$ occurs $|S|/2^m = 2^{n-k-m} - 1$ times because for each $u_2 \in S$, we can choose $u_1 \in \mathbb{F}_2^n$ such that $u_1 = \mathbf{1} + u_2$, and the multiplicity for each non-zero weight is 2^m by Lemma 3.1. In this way, we can compute the frequency for each non-zero weight. □

TABLE 1. $wd(\mathcal{C}_D(\mathbb{F}_2;\mathbb{F}_2^{2n+1}))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) \leq n-m-2$.

i	A_i
0	1
$2^{n+k}-2^n$	1
$2^{2n-m-1}-2^{n+k}+2^n-1$	$2^{n-k-m}-1$
$2^{2n-m-1}-2^n$	$2^{n-m}-2^{n-k-m}$
$2^{2n-m-1}-1$	$2^{2n-m+1}-2^{n-m}-1$
2^{2n-m-1}	$2^{2n-m+1}-2^{n-m}-1$
$2^{2n-m-1}+2^n-1$	$2^{n-m}-2^{n-k-m}$
$2^{2n-m-1}+2^{n+k}-2^n$	$2^{n-k-m}-1$
$2^{2n-m}-2^{n+k}+2^n-1$	1
$2^{2n-m}-1$	1

TABLE 2. $wd(\mathcal{C}_D(\mathbb{F}_2;\mathbb{F}_2^{2n+1}))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) = n-m-1$ or $k = n-m$.

i	0	2^n-1	$2^{2n-m-1}-2^n$	$2^{2n-m-1}-1$
A_i	1	1	$2^{n-m}-1$	$2^{2n-m+1}-2^{n-m}-1$
i	2^{2n-m-1}	$2^{2n-m-1}+2^n-1$	$2^{2n-m}-2^n$	$2^{2n-m}-1$
A_i	$2^{2n-m+1}-2^{n-m}-1$	$2^{n-m}-1$	1	1

TABLE 3. $wd(\mathcal{C}_D(\mathbb{F}_2;\mathbb{F}_2^{2n+1}))$ with $\lambda^{-1}(1) = H_m \setminus C$ when $\dim(C) \leq n-m-2$ except zero and all-ones vectors.

i	$2^{n+k}-1$	$2^{2n-m-1}-2^{n+k}$	$2^{2n-m-1}-1$
A_i	1	$2^{n-k-m}-1$	$2^{2n-m+1}-2^{n-m-k}-1$
i	2^{2n-m-1}	$2^{2n-m-1}+2^{n+k}-1$	$2^{2n-m}-2^{n+k}$
A_i	$2^{2n-m+1}-2^{n-m-k}-1$	$2^{n-k-m}-1$	1

We finally consider the case where D is the complement of a Vasil'ev code. We only state the result without proof since the arguments are similar to those of the previous lemma.

Lemma 3.3. *Let H_m be the Hamming code of length $n = 2^m - 1$ for $m \geq 2$ and D a Vasil'ev code corresponding to a nonlinear function λ on H_m. Let C be a linear subcode of H_m. Let $W = \mathbb{F}_2$ and $V = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$.*

(1) *Set $\lambda^{-1}(1) = C^*$, where $\dim(C) = k$.*
Then $\mathcal{C}_{D^c}(W;V)$ is a linear code with parameters $[2^{2n+1}-2^{2n-m}, 2n+2, 2^{2n}-2^{2n-m}]$.
If $1 \leq k \leq n-m-2$, then it is ten-weight whose weight distribution is given by Table 4.

TABLE 4. $wd(\mathcal{C}_{D^c}(\mathbb{F}_2;\mathbb{F}_2^{2n+1}))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) \leq n-m-2$.

i	A_i
0	1
$2^{2n}-2^{2n-m}$	2^m-1
$2^{2n}-2^{2n-m}+2^{n+k}-2^n$	2^m
$2^{2n}-2^{2n-m-1}-2^{n+k}+2^n$	$2^{n-k}-2^m$
$2^{2n}-2^{2n-m-1}-2^n$	2^n-2^{n-k}
$2^{2n}-2^{2n-m-1}$	$2^{2n+1}-2^n-2^m$
$2^{2n}-2^{2n-m-1}+2^n$	2^n-2^{n-k}
$2^{2n}-2^{2n-m-1}+2^{n+k}-2^n$	$2^{n-k}-2^m$
$2^{2n}-2^{n+k}+2^n$	2^m
2^{2n}	2^m-1
$2^{2n+1}-2^{2n-m}$	1

TABLE 5. $wd(\mathcal{C}_{D^c}(\mathbb{F}_2;\mathbb{F}_2^{2n+1}))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) = n-m-1$.

i	A_i
0	1
$2^{2n}-2^{2n-m}$	2^m-1
$2^{2n}-2^{2n-m}+2^n$	2^m
$2^{2n}-2^{2n-m-1}-2^n$	2^n-2^m
$2^{2n}-2^{2n-m-1}$	$2^{2n+1}-2^n-2^m$
$2^{2n}-2^{2n-m-1}+2^n$	2^n-2^m
$2^{2n}-2^n$	2^m
2^{2n}	2^m-1
$2^{2n+1}-2^{2n-m}$	1

If k is either $n-m-1$ or $n-m$, then it is eight-weight whose wight distribution is given by Table 5.

(2) *Set $\lambda^{-1}(1) = H_m \setminus C$, where $\dim(C) = k$.*
If $1 \leq k \leq n-m-2$, then $\mathcal{C}_{D^c}(W;V)$ is an eight-weight linear code with parameters $[2^{2n+1}-2^{2n-m}, 2n+2, 2^{2n}-2^{2n-m}]$ whose weight distribution is given by Table 6.

4. Two- or three-weight linear codes

In this section, we construct several classes of two- or three-weight linear codes from Vasil'ev codes.

TABLE 6. $wd(\mathcal{C}_{D^c}(\mathbb{F}_2; \mathbb{F}_2^{2n+1}))$ with $\lambda^{-1}(1) = H_m \setminus C$ when $\dim(C) \leq n-m-2$.

i	A_i
0	1
$2^{2n} - 2^{2n-m}$	$2^m - 1$
$2^{2n} - 2^{2n-m} + 2^{n+k}$	2^m
$2^{2n} - 2^{2n-m-1} - 2^{n+k}$	$2^{n-k} - 2^m$
$2^{2n} - 2^{2n-m-1}$	$2^{2n+1} - 2^{n-k} - 2^m$
$2^{2n} - 2^{2n-m-1} + 2^{n+k}$	$2^{n-k} - 2^m$
$2^{2n} - 2^{n+k}$	2^m
2^{2n}	$2^m - 1$
$2^{2n+1} - 2^{2n-m}$	1

TABLE 7. $wd(\mathcal{C}_D(\mathbb{F}_2; \mathbb{F}_2^n \times \mathbb{F}_2^n \times \{0\}))$

i	0	$2^{2n-m-1} - 1$	2^{2n-m-1}	$2^{2n-m} - 1$
A_i	1	$2^{2n-m} - 1$	$2^{2n-m} - 1$	1

Proposition 4.1. *Let H_m be the Hamming code of length $n = 2^m - 1$ for $m \geq 2$ and D a Vasil'ev code associated with the Hamming code H_m. Let W be a subspace of $\mathbb{F}_2$ and V a subspace of $\mathbb{F}_2^{2n+1}$.*

(i) *If $(W, V) = (\{0\}, \mathbb{F}_2^n \times \mathbb{F}_2^n \times \{0\})$, then $\mathcal{C}_D(W; V)$ is an one-weight linear code with parameters $[2^{2n-m} - 1, 2n - m, 2^{2n-m-1}]$. In particular, the code is optimal in the sense that it attains the Griesmer bound.*

(ii) *If $(W, V) = (\mathbb{F}_2, \mathbb{F}_2^n \times \mathbb{F}_2^n \times \{0\})$, then $\mathcal{C}_D(W; V)$ is a three-weight linear code with parameters $[2^{2n-m} - 1, 2n - m + 1, 2^{2n-m-1} - 1]$ and the weight distribution is given by Table 7. The code is optimal in the sense that it attains the Grey-Rankin bound.*

Proof. (i) According to Lemma 3.1, the dimension of $\mathcal{C}_D(W; V)$ is $2n - m$. Let $c_D(s, u) = c_D(s, (u_1|u_2|0))$ be in $\mathcal{C}_D(W; V)$. Then in (6), the weight of $c_D(s, u)$ equals

$$\mathrm{wt}(c_D(s, u)) = 2^{2n-m-1} - 2^{2n-m-1} \mathbb{1}_{H_m^\perp}(u_2) \times \delta_{u_1, u_2},$$

which does not depend on the choice of λ. It follows that non-zero weight is only 2^{2n-m-1}, and the frequency for the weight is easily computed. Finally, it can be seen that for $\mathcal{C}_D(V; W)$

$$\sum_{i=0}^{(2n-m)-1} \left\lceil \frac{2^{2n-m-1}}{2^i} \right\rceil = 2^{2n-m-1} + 2^{2n-m-2} + \cdots + 2 + 1 = 2^{2n-m} - 1,$$

hence it attains the Griesmer bound.

(ii) According to Lemma 3.1, the dimension of $\mathcal{C}_D(W; V)$ is $2n - m + 1$. Let $c_D(s, u) = c_D(s, (u_1|u_2|0))$ be in $\mathcal{C}_D(W; V)$. Then in (3), the weight of $c_D(s, u)$

TABLE 8. $wd(\mathcal{C}_D(\{0\}; \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) = n - m - 1$ or $k = n - m$.

i	0	$2^{2n-m-1} - 2^n$	2^{2n-m-1}	$2^{2n-m} - 2^n$
A_i	1	$2^{n-m} - 1$	$2^{2n-m+1} - 2^{n-m} - 1$	1

TABLE 9. $wd(\mathcal{C}_D(\{0\}; \mathbb{F}_2^n \times H_m^\perp \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) \le n - m - 1$.

i	0	$2^{n+k} - 2^n$	2^{2n-m-1}
A_i	1	1	$2^{n+1} - 2$

TABLE 10. $wd(\mathcal{C}_{D^c}(\{0\}; \mathbb{F}_2^n \times H_m^\perp \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) \le n - m - 1$.

i	0	$2^{2n} - 2^{2n-m-1}$	$2^{2n} - 2^{n+k} + 2^n$	2^{2n}
A_i	1	$2^{n+m+1} - 2^{m+1}$	2^m	$2^m - 1$

TABLE 11. $wd(\mathcal{C}_D(\{0\}; \mathbb{F}_2^n \times C^\perp \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) = n - m$.

i	0	2^{2n-m-1}	$2^{2n-m} - 2^n$
A_i	1	$2^{n+m+1} - 2$	1

equals

$$\mathrm{wt}(c_D(s,u)) = \frac{1}{2}(|D^*| + (-1)^s) - \frac{(-1)^s}{2} 2^n \delta_{u_1,u_2} \times 2^{n-m} \mathbb{1}_{H_m^\perp}(u_2),$$

which does not depend on the choice of λ. It follows that non-zero weights are $2^{2n-m-1} - 1, 2^{2n-m-1}, 2^{2n-m} - 1$, and the frequency for each weight is computed as in Lemma 3.2. To prove the optimality, let's denote n_c, k_c and d_c as the length, dimension and minimum weight of the code. Since $n_c - 2d_c = 1$, $n_c - d_c = 2^{2n-m-1}$, we have

$$\frac{8d_c(n_c - d_c)}{n_c - (n_c - 2d_c)^2} = \frac{8(2^{2n-m-1} - 1)2^{2n-m-1}}{2^{2n-m} - 2} = 2^{2n-m+1} = 2^{k_c},$$

so that it can be proven that the optimality follows from (2). □

Remark 4.2. The parameters of codes constructed in Proposition 4.1 are well known and can be derived by other means. The linear codes in Proposition 4.1(i) is equivalent to the simplex code, and the linear code in Proposition 4.1(ii) is equivalent to the punctured first-order Reed-Muller code because any linear code with parameters $[2^N, N + 1, 2^{N-1}]$ for $N \ge 1$ is unique [4].

The following two theorems are direct consequences of Lemmas 3.2 and 3.3.

TABLE 12. $wd(\mathcal{C}_{D^c}(\{0\};\mathbb{F}_2^n \times C^\perp \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = C^*$ when $\dim(C) = n - m$.

i	0	$2^{2n} - 2^{2n-m} + 2^n$	$2^{2n} - 2^{2n-m-1}$	2^{2n}
A_i	1	2^m	$2^{n+m+1} - 2^{m+1}$	$2^m - 1$

Theorem 4.3. *Let H_m be the Hamming code of length $n = 2^m - 1$ for $m \geq 2$ and D a Vasil'ev code corresponding to a nonlinear function λ on H_m of which $\lambda^{-1}(1) = C^*$, where C is a linear subcode of H_m with dimension k. Let $W = \{0\}$ be a trivial subspace of $\mathbb{F}_2$ and V a subspace of $\mathbb{F}_2^{2n+1}$.*

(i) $1 \leq k \leq n - m - 1$;

(1) *If $V = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$ and $k = n-m-1$, then $\mathcal{C}_D(W;V)$ is a three-weight linear code with parameters $[2^{2n-m} - 1, 2n - m + 1, 2^{2n-m-1} - 2^n]$ and its weight distribution is given by Table 8.*

(2) *If $V = \mathbb{F}_2^n \times H_m^\perp \times \mathbb{F}_2$ and $k < n-m-1$, then $\mathcal{C}_D(W;V)$ is a two-weight linear code with parameters $[2^{2n-m} - 1, n + 1, 2^{n+k} - 2^n]$ and $\mathcal{C}_{D^c}(W;V)$ is a three-weight linear code with parameters $[2^{2n+1} - 2^{2n-m}, n + m + 1, 2^{2n} - 2^{2n-m-1}]$. Their weight distributions are given by Tables 9 and 10. Furthermore, these codes are minimal. The code in Table 10 satisfies AB-condition and the code in Table 9 does not satisfy AB-condition, but it satisfies DHZ-condition.*

(ii) $k = n - m$;

(1) *If $V = \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$, then $\mathcal{C}_D(W;V)$ is a three-weight linear code with parameters $[2^{2n-m} - 1, 2n - m + 1, 2^{2n-m-1} - 2^n]$ and its weight distribution is given by Table 8.*

(2) *If $V = \mathbb{F}_2^n \times H_m^\perp \times \mathbb{F}_2$, then $\mathcal{C}_D(W;V)$ is a two-weight linear code with parameters $[2^{2n-m} - 1, n + m + 1, 2^{2n-m-1}]$ and $\mathcal{C}_{D^c}(W;V)$ is a three-weight linear code with parameters $[2^{2n+1} - 2^{2n-m}, n + m + 1, 2^{2n} - 2^{2n-m} + 2^n]$. Their weight distributions are given by Tables 11 and 12. Furthermore, these codes are minimal since they satisfy AB-condition.*

Proof. We just provide the proof of (i)-2. By Lemma 3.1, the dimensions of $\mathcal{C}_D(\{0\};\mathbb{F}_2^n \times C^\perp \times \mathbb{F}_2)$ is $2n-m-k+1$. The frequency for each non-zero weight can be computed by using the same arguments as Lemma 3.2. Finally we check the minimality. In Table 9, we have $w_1 = 2^{n+k} - 2^n$ and $w_2 = 2^{2n-m-1}$. Since $k < n - m - 1$, it follows that

$$\frac{2^{n+k} - 2^n}{2^{2n-m-1}} < \frac{1}{2},$$

and hence this code does not satisfy AB-condition. Furthermore, since $2w_1 = 2(2^{n+k} - 2^n) \neq 2^{2n-m-1} = w_2$, this code satisfies DHZ-condition, hence it is minimal. □

TABLE 13. $wd(\mathcal{C}_D(\{0\};\mathbb{F}_2^n\times H_m^\perp\times\mathbb{F}_2))$ with $\lambda^{-1}(1)=H_m\backslash C$ when $\dim(C)\le n-m-2$.

i	0	2^{2n-m-1}	$2^{2n-m}-2^{n+k}$
A_i	1	$2^{n+1}-2$	1

TABLE 14. $wd(\mathcal{C}_{D^c}(\{0\};\mathbb{F}_2^n\times H_m^\perp\times\mathbb{F}_2))$ with $\lambda^{-1}(1)=H_m\backslash C$ when $\dim(C)\le n-m-2$.

i	0	$2^{2n}-2^{2n-m}+2^{n+k}$	$2^{2n}-2^{2n-m-1}$	2^{2n}
A_i	1	2^m	$2^{n+m+1}-2^{m+1}$	2^m-1

Remark 4.4. As it is remarked in [6], the construction of an infinite family of binary minimal linear codes which does not satisfy AB-condition is a hard problem in general. The code $\mathcal{C}_D(W;V)$ in Theorem 4.3 with $k<n-m-1$ gives another such an infinite family. We refer to [3, 6] for previously known such families.

Theorem 4.5. *Let H_m be the Hamming code of length $n=2^m-1$ for $m\ge 2$ and D a Vasil'ev code corresponding to a nonlinear function λ on H_m of which $\lambda^{-1}(1)=H_m\setminus C$, where C is a linear subcode of H_m with dimension k for $1\le k\le n-m-2$. If $(W,V)=(\{0\},\mathbb{F}_2^n\times H_m^\perp\times\mathbb{F}_2)$, then $\mathcal{C}_D(W;V)$ is a two-weight linear code with parameters $[2^{2n-m}-1,n+1,2^{2n-m-1}]$ and $\mathcal{C}_{D^c}(W;V)$ is a three-weight linear code with parameters $[2^{2n+1}-2^{2n-m},n+m+1,2^{2n}-2^{2n-m}+2^{n+k}]$. Their weight distributions are given by Tables 13 and 14. Furthermore, these codes are minimal since they satisfy AB-condition.*

We close this section with a simple example.

Example 4.6. (i) Let $C=H_3\cap\mathbb{E}_2^7$. Consider the Vasil'ev code D associated with $\lambda^{-1}(1)=C^*$ which is of length 15 and of size 2^{11}. Then the dimension of C is three and it is generated by

$$\{1100110,1010101,0001111\}.$$

Its dual code $C^\perp$ is generated by C and 1100011. By Theorem 4.3, we obtain that $\mathcal{C}_D(\{0\};\mathbb{F}_2^7\times\mathbb{F}_2^7\times\mathbb{F}_2)$ has the weight enumerator $1+15z^{896}+4079z^{1024}+z^{1920}$,

$\mathcal{C}_D(\{0\};\mathbb{F}_2^7\times H_3\times\mathbb{F}_2)$ has the weight enumerator $1+254z^{1024}+z^{1920}$ and

$\mathcal{C}_{D^c}(\{0\};\mathbb{F}_2^7\times H_3\times\mathbb{F}_2)$ has the weight enumerator $1+8z^{14464}+2032z^{15360}+7z^{16384}$.

(ii) Let $C=\{\mathbf{0}\}$ be the trivial subcode of H_3. Consider the Vasil'ev code D associated with $\lambda^{-1}(1)=H_3^*$. By Theorem 4.5, we obtain that

$\mathcal{C}_D(\{0\};\mathbb{F}_2^7\times H_3\times\mathbb{F}_2))$ has the weight enumerator $1+255z^{896}+z^{1024}$ and

$\mathcal{C}_{D^c}(\{0\}; \mathbb{F}_2^7 \times H_3 \times \mathbb{F}_2))$ has the weight enumerator $1 + 8z^{14976} + 2032z^{15360} + 7z^{16384}$.

Acknowledgments. We express our gratitude to a reviewer for his/her very helpful comments, which improved the exposition of this paper, and wish to thank Prof. Hyun Kwang Kim for his valuable suggestions and proofreading of this paper.

References

[1] A. Ashikhmin and A. Barg, *Minimal vectors in linear codes*, IEEE Trans. Inform. Theory **44** (1998), no. 5, 2010–2017. https://doi.org/10.1109/18.705584

[2] R. Calderbank and W. M. Kantor, *The geometry of two-weight codes*, Bull. London Math. Soc. **18** (1986), no. 2, 97–122. https://doi.org/10.1112/blms/18.2.97

[3] S. Chang and J. Y. Hyun, *Linear codes from simplicial complexes*, Des. Codes Cryptogr. **86** (2018), no. 10, 2167–2181. https://doi.org/10.1007/s10623-017-0442-5

[4] Y. Chen and A. J. H. Vinck, *A lower bound on the optimum distance profiles of the second-order Reed-Muller codes*, IEEE Trans. Inform. Theory **56** (2010), no. 9, 4309–4320. https://doi.org/10.1109/TIT.2010.2054512

[5] G. D. Cohen, S. Mesnager, and A. Patey, *On minimal and quasi-minimal linear codes*, in Cryptography and coding, 85–98, Lecture Notes in Comput. Sci., 8308, Springer, Heidelberg, 2013. https://doi.org/10.1007/978-3-642-45239-0_6

[6] C. Ding, Z. Heng, and Z. Zhou, *Minimal binary linear codes*, IEEE Trans. Inform. Theory **64** (2018), no. 10, 6536–6545. https://doi.org/10.1109/TIT.2018.2819196

[7] C. Ding and J. Yuan, *Covering and secret sharing with linear codes*, in Discrete mathematics and theoretical computer science, 11–25, Lecture Notes in Comput. Sci., 2731, Springer, Berlin, 2003. https://doi.org/10.1007/3-540-45066-1_2

[8] T. Etzion and A. Vardy, *Perfect binary codes: constructions, properties, and enumeration*, IEEE Trans. Inform. Theory **40** (1994), no. 3, 754–763. https://doi.org/10.1109/18.335887

[9] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes. I*, North-Holland Publishing Co., Amsterdam, 1977.

[10] G. McGuire, *Quasi-symmetric designs and codes meeting the Grey-Rankin bound*, J. Combin. Theory Ser. A **78** (1997), no. 2, 280–291. https://doi.org/10.1006/jcta.1997.2765

[11] Ju. L. Vasil'ev, *On ungrouped, close-packed codes*, Problemy Kibernet. No. **8** (1962), 337–339.

Jong Yoon Hyun
Konkuk University, Glocal Campus
Chungju-si 27478, Korea
Email address: hyun33@kku.ac.kr

Jaeseon Kim
CRYPTO LAB INC.
404, 27, 1, Gwanak-ro, Gwanak-gu, Seoul 08826, Korea
Email address: arkenkjs@postech.ac.kr