Construction of two- or three-weight binary linear codes from Vasil'ev codes

Jaeseon, Kim

(Joint work with Hyun Kwang Kim and Jong Yoon Hyun)

Department of Mathematics, POSTECH

2018 Sino-Korea conference on Coding Theory and Its related Topics

Shanghai University

July 4, 2018

Basic Notaion about Linear Algebra

- $\mathbb{F}_2 :=$ A field of consisting two elements 0 and 1.
- $\mathbb{F}_2^n :=$ A vector space of dimension n over $\mathbb{F}_2$.
- For $D \subset \mathbb{F}_2^n$,

$$D^* := D \setminus \{\mathbf{0}\} \text{ and } D^c := \mathbb{F}_2^n \setminus D$$

  where $\mathbf{0}$ is the zero vector of $\mathbb{F}_2^n$.
- $\mathrm{rank}(D) :=$ the dimension of the linear space $\langle D \rangle$ generated by D over $\mathbb{F}_2$.
- $D^\perp := \{x \in \mathbb{F}_2^n | x \cdot y = 0 \text{ for all } y \in D\}$: the dual space of D where $\cdot$ is the usual inner product on $\mathbb{F}_2^n$.

Well-Known Fact

For $D \subset \mathbb{F}_2^n$, $D^\perp$ is a linear space of $\mathbb{F}_2$ and $\dim(D^\perp) = n - \mathrm{rank}(D)$.

Basic Notaion about Coding Theory (i)

- For $x = (x_1, x_2, \ldots, x_n) \in \mathbb{F}_2^n$, the Hamming weight of x is defined by

$$\mathrm{wt}(x) = \#\{i \in \{1, 2, \ldots, n\} | x_i \neq 0\}$$

- A (n, M, d)-code C is a subset of $\mathbb{F}_2^n$ with size M and the minimum distance $d = \min\{\mathrm{wt}(x - y) | x, y \in C, x \neq y\}$. The vectors in C is called codewords.
- A $[n, k, d]$-linear code C is a linear space of $\mathbb{F}_2^n$ with dimension k and the minimum weight $d = \min\{\mathrm{wt}(x) | x \in C^*\}$.
- $\{A_i(C)\}_{i=0}^n$ is called the weight distribution of C where $A_i(C) := \#\{x \in C | \mathrm{wt}(x) = i\}$.

Definition

A linear code C is called a t-weight code if the number of non-zero $A_i(C)$ in $\{A_i\}_{i \geq 1}$ is equal to t.

Basic Notaion about Coding Theory (*ii*)

- A (n, k, d)-code C is a perfect if $2^n = |C| \times \sum_{i=0}^{\lfloor \frac{d}{2} \rfloor} \binom{n}{i}$.
- For a $[n, k, d]$-linear code C, there is an $(n-k) \times n$ matrix H such that

$$C = \{x \in \mathbb{F}_2^n | Hx^t = \mathbf{0}\}.$$

  H is called a parity check matrix for C.
- Let $n = 2^m - 1$ with $m \geq 3$. Then $m \times (2^m - 1)$ matrix H whose columns are the numbers $1, 2, \ldots, 2^m - 1$ written as binary expressions, is the parity check matrix for an $[n = 2^m - 1, n - m, 3]$ linear code H_m. H_m is called the Hamming code of length $n = 2^m - 1$.

Basic Notaion about Coding Theory (*iii*)

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

Definition of Vasil'ev codes

Define a code of $\mathbb{F}_2^{2n+1}$ as follows :

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

Then D is a $(2n+1, 2^{2n-m}, 3)$-perfect code whose rank become

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

The code D is called a Vasil'ev code with respect to H_m (or with respect to λ).

The definition of $\mathcal{C}_D(V; W)$

Definition

Let $D \subset \mathbb{F}_2^n$ where $n \geq 1$. Define the code as follows:

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

where V and W are subspaces of $\mathbb{F}_2$ and $\mathbb{F}_2^n$, respectively. We call D the defining set of $\mathcal{C}_D(V; W)$.

- $\mathcal{C}_D(V; W)$ is a linear code of length $|D^*|$ and dimension at most $\dim(V) + \dim(W)$.
- Note that $\mathcal{C}_D(\mathbb{F}_2; W)$ is a self-complementary, indeed, $\mathcal{C}_D(\mathbb{F}_2; W) = \mathcal{C}_D(\{\mathbf{0}\}; W) \dot{\cup} (\mathbf{1} + \mathcal{C}_D(\{\mathbf{0}\}; W))$.

Dimension Lemma

Dimension Lemma

Let H_m be the Hamming code of length $n = 2^m - 1$ for $m \geq 3$ and D a Vasil'ev code associated with the Hamming code H_m. Let V be a subspace of $\mathbb{F}_2$ and W a subspace of $\mathbb{F}_2^{2n+1}$. The the following statements are true.

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

Computation of weight of $c(s,u)$ (i)

- For each $c(s,u) \in \mathcal{C}_D(\mathbb{F}_2; \mathbb{F}_2^n)$, the nullity of $c_D(s,u)$ define as follows:

$$N(s,u) := |\{x \in D^* | s + u \cdot x = 0\}| \text{ so that}$$

$$2N(s,u) = \sum_{x \in D^*} \sum_{y \in \mathbb{F}_2} (-1)^{y(s+u\cdot x)} = |D^*| + (-1)^s \sum_{x \in D^*} (-1)^{u \cdot x}.$$

- The weight of $c_D(s,u)$ is given by

$$\text{wt}(c_D(s,u)) = |D^*| - N(s,u) = \frac{1}{2}|D^*| - \frac{(-1)^s}{2}\chi_u(D),$$

  where $\chi_u(D) = \sum_{x \in D^*} (-1)^{u \cdot x}$.

- Let $x = (x_1 | x_1 + x_2 | \pi(x_1) + \lambda(x_2)) \in D$ and $u = (u_1 | u_2 | t) \in \mathbb{F}_2^n \times \mathbb{F}_2^n \times \mathbb{F}_2$. Then the weight of $c_D(s,u)$ and $c_{D^c}(s,u)$ computed as follows:

Computation of weight of $c(s,u)$ (ii)

weight of $c_D(s,u)$

The weight of $c_D(s,u)$ is given by

$$\frac{1}{2}(|D^*|+(-1)^s)-\frac{(-1)^s}{2}\left(2^{n-1}\mathbb{1}_{\langle \mathbf{1}\rangle}(u_1+u_2)+(-1)^t(2^n\delta_{u_1,u_2}-2^{n-1}\mathbb{1}_{\langle \mathbf{1}\rangle}(u_1+u_2))\right) \times \left(2^{n-m}\mathbb{1}_{H_m^\perp}(u_2)-2t\chi_{u_2}(\lambda^{-1}(1))\right)$$

where $\mathbb{1}_S(x)$ is the indicator function of a set S.

weight of $c_{D^c}(s,u)$

The weight of $c_{D^c}(s,u)$ is given by

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

Computation of weight of $c(s, u)$ (iii)

To compute explicitly the weights in two codes, it is required a suitable choice of the non-linear function λ. We consider two cases as follows:

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

We set $\lambda^{-1}(1) = C^*$, where C is a linear subcode in H_m with dimension $k \geq 1$. Then

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

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

We set $\lambda^{-1}(1) = H_m \setminus C$, where C is a linear subcode in H_m with dimension $1 \leq k \leq n - m - 2$. Then

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

Well-known Bounds

Theorem (the Griesmer bound)

For a $[n, k, d]$-linear code C, the following inequality holds:

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

Theorem (the Grey-Rankin bound)

For any $[n, k, d]$-self-complementary linear code C, the following inequality holds:

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

Here, a linear code is called a self-complement code if it contains all-ones vector.

Two- or three-weight linear codes(i)

Theorem

Let H_m be the Hamming code of length $n = 2^m - 1$ for $m \geq 3$ and D a Vasil'ev code associated with the Hamming code H_m.

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

Table: $wd(\mathcal{C}_{D^c}(\{0\}; \mathbb{F}_2^n \times \mathbb{F}_2^n \times \{0\}))$, the Griesmer bound

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

Table: $wd(\mathcal{C}_D(\mathbb{F}_2; \mathbb{F}_2^n \times \mathbb{F}_2^n \times \{0\}))$, the Grey-Rankin bound

Minimal code

Minimal code

A codeword c in a linear code C is said to be minimal if there is no codeword in C whose support is contained in the support of c. A linear code C is said to be minimal if every codeword in C is minimal.

- Well-known facts that a linear code C is minimal if $W_{min}/W_{max} > 1/2$, where W_{min} and W_{max} denote the minimum and maximum nonzero weights in C, respectively.
- C.Ding et al. present a new condition for a binary linear code to be minimal. (c.f.) C. Ding, Z. Heng, Z. Zhou, Minimal Binary Linear Codes, IEEE Trans. Inf. Theory (2018))

Two- or three-weight linear codes(ii)

Theorem

Let $\lambda : H_m \to \mathbb{F}_2$ be a function such that $\lambda^{-1}(1) = C^*$ where C is a linear subcode of H_m with dimension k.

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: $wd(\mathcal{C}_{D^c}(\{0\}; \mathbb{F}_2^n \times H_m^{\perp} \times \mathbb{F}_2))$, $W_{min}/W_{max} > 1/2$.

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

Table: $wd(\mathcal{C}_D(\{0\}; \mathbb{F}_2^n \times H_m^{\perp} \times \mathbb{F}_2))$, $W_{min}/W_{max} < 1/2$ if $k \geq n - m - 2$.

Two- or three-weight linear codes(*iii*)

Theorem (Continue)

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

Table: $wd(\mathcal{C}_D(\{0\};\mathbb{F}_2^n \times C^\perp \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = H_m^*$, $W_{min}/W_{max} < 1/2$.

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

Table: $wd(\mathcal{C}_{D^c}(\{0\};\mathbb{F}_2^n \times C^\perp \times \mathbb{F}_2))$ with $\lambda^{-1}(1) = H_m^*$, $W_{min}/W_{max} < 1/2$.

Two- or three-weight linear codes(iv)

Theorem

Let $\lambda : H_m \to \mathbb{F}_2$ *such that* $\lambda^{-1}(1) = H_m \setminus C$, *where* C *is a linear subcode of* H_m *with dimension* k *for* $1 \leq k \leq n - m - 2$.

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

Table: $wd(\mathcal{C}_D(\{0\}; \mathbb{F}_2^n \times H_m^{\perp} \times \mathbb{F}_2))$, $W_{min}/W_{max} > 1/2$.

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

Table: $wd(\mathcal{C}_{D^c}(\{0\}; \mathbb{F}_2^n \times H_m^{\perp} \times \mathbb{F}_2))$, $W_{min}/W_{max} < 1/2$.