Linear codes constructed from simplicial complexes

The 5th Sino-Korea International Conference on Coding theory and Its Related Topics

July 2-6 2018

Jong Yoon Hyun

(joint work with Seunghwan Chang)

KIAS

Outline

1. Minimal linear codes
2. Simplicial complexes and their generating functions
3. Construction a family of minimal linear codes from simplicial complexes violating Ashikhmin-Barg condition

Minimal linear codes

- C is a binary linear code
- Throughout all slides we identify a vector with its support
- A non-zero codeword u of C is minimal if v is a subset of u implies v=u
- A linear code is minimal if every non-zero codeword of C is minimal

(If and only if C is an intersecting code)

A sufficient condition to be minimal

Ashikhmin-Barg, 1998

A linear code is minimal if $\frac{d_{min}}{d_{max}} > \frac{1}{2}$ (A-B condition)

Linear codes from a defining set

D is a subset of F_q

$$C_D = \{\big(Tr(\alpha x)\big)_{\alpha \in D} : x \in F_q\}$$

This linear code is introduced by Ding-Ding

Ding K., Ding C, A class of two-weight and three-weight codes, and their applications in secret sharing, IEEE Trans. Inf. Theory **61**, 5835–5842 (2015)

There are many constructions of few-weight minimal linear codes from C_D or its variants using A-B condition

A linear code is minimal if $\frac{d_{min}}{d_{max}} > \frac{1}{2}$ (A-B condition)

A minimal linear code violating A-B condition

Cohen-Mesnager-Patey,
On minimal and quasi-minimal linear codes, Cryptography and coding. Lecture Notes In IMA International Conference on Cryptography and Coding, vol. 8308, pp. 85-98. Springer, Heidelberg (2013)

They provide **only one example** of minimal linear code violating A-B condition

Ashikhmin-Barg, 1998

A linear code is minimal if $\frac{d_{min}}{d_{max}} > \frac{1}{2}$ (A-B condition)

In this talk

Construction **a family of** minimal linear codes violating A-B condition using simplicial complexes

Seunghwan Chang, Jong Yoon Hyun, Linear codes from simplicial complexes, (2018) Designs, Codes and Cryptography, https://doi.org/10.1007/s10623-017-0442-5

A linear code is minimal if $\frac{d_{min}}{d_{max}} > \frac{1}{2}$ (A-B condition)

It seems that ½ is a threshold between combinatorics and number theory

Simplicial complexes

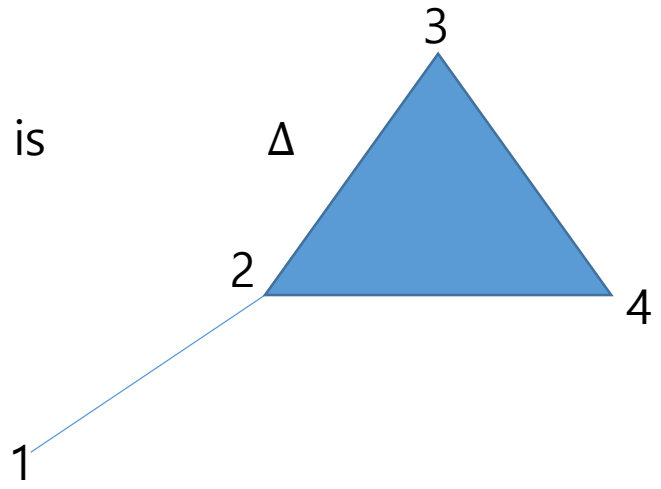
■ Z_2^n is the set of binary n-tuples

■ A subset Δ of Z_2^n is a simplicial complex if u in Δ and v is a subset of u imply v in Δ

Example

The simplicial complex Δ generated by {1,2}, {2,3,4} is

{∅, {1}, {2}, {1,2}, {3}, {4}, {2,3}, {2,4}, {3,4}, {2,3,4}}



The generating function of a simplicial complex

Let Δ be a simplicial complex of Z_2^n.

$$\sum_{u \in \Delta} x^{|u|} y^{n-|u|}$$

The simplicial complex Δ generated by {1,2}, {2,3,4} is

{∅, {1}, {2}, {1,2}, {3}, {4}, {2,3}, {2,4}, {3,4}, {2,3,4}}

$$\sum_{u \in \Delta} x^{|u|} y^{n-|u|} = y^4 + 4xy^3 + 4x^2y^2 + x^3y$$

The generating function of a simplicial complex

FACT (Adamaszek, 2015)

Let Δ be a simplicial complex of Z_2^n. Then

$$\sum_{u \in \Delta} x^{|u|} y^{n-|u|} = \sum_{\emptyset \neq S \subseteq \mathcal{F}} (-1)^{|S|+1} (x+y)^{|\cap S|} y^{n-|\cap S|}$$

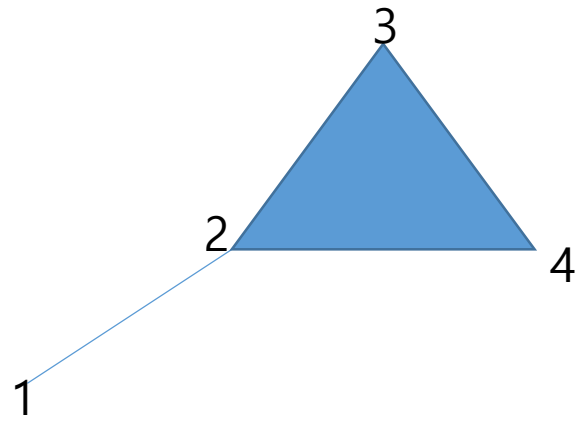
where F is the set of maximal elements

The multivariable generating function of a simplicial complex

Let Δ be a simplicial complex of Z_2^n. Then

$$\mathcal{H}_\Delta(x_1, x_2, \ldots, x_n) = \sum_{u \in \Delta} \prod_{i=1}^{n} x_i^{u_i} \in \mathbb{Z}[x_1, \ldots, x_n].$$

Example



$$H_{\Delta}(x_1, x_2, \ldots, x_4) = 1 + x_1 + x_2 + x_3 + x_4 + x_1x_2 + x_2x_3 + x_2x_4 + x_3x_4 + x_2x_3x_4$$

The multivariable generating function of a simplicial complex

Theorem (Chang-H, 2018)

Let Δ be a simplicial complex of Z_2^n. Then

$$\mathcal{H}_\Delta(x_1, \ldots, x_n) = \sum_{\emptyset \neq S \subseteq \mathcal{F}} (-1)^{|S|+1} \prod_{i \in \cap S} (1 + x_i)$$

where F is the set of maximal elements

Linear codes from a defining set

For a subset D of Z_2^n, we define

$$C_D = \{(u \cdot x)_{x \in D} : u \in Z_2^n\}$$

Then it is a linear code of length |D| and dimension at most n

We can construct infinite families of distance optimal linear codes from C_{Δ^c}, where Δ is a simplicial complex (J. Y. Hyun, J. Lee, Y. Lee)

Linear codes from simplicial complexes

A Boolean function f is a function from Z_2^n to Z_2

Let f be a non-linear Boolean function in n variables with f(0)=0

$$C_f = \{c_f(s,u) = (sf(x) + u \cdot x)_{x \in \mathbb{Z}_2^{n*}} : s \in \mathbb{Z}_2, u \in \mathbb{Z}_2^n\}$$

(introduced by C. Carlet, C. Ding, Wadayama et al)

Then C_f is a linear code of length $2^n - 1$ and dimension n+1

Take $f^{-1}(1)$ to be a simplicial complex $\Delta \setminus \{0\}$

The Hamming weight of $c_f(s,u)$

$$C_f = \{c_f(s,u) = (sf(x) + u \cdot x)_{x \in \mathbb{Z}_2^{n*}} : s \in \mathbb{Z}_2, u \in \mathbb{Z}_2^n\}$$

$$\begin{aligned} w_H(c_f(s,u)) &= 2^{n-1} - 1 - \sum_{x \in \mathbb{Z}_2^{n*}} \delta_{0,sf(x)+u \cdot x} \\ &= 2^{n-1} - 1 - \frac{1}{2} \sum_{y \in \mathbb{Z}_2} \sum_{x \in \mathbb{Z}_2^{n*}} (-1)^{y(sf(x)+u \cdot x)} \\ &= 2^{n-1} - \frac{1}{2} S_{sf}(u) \end{aligned}$$

Walsh-Hadamard transform

- A Boolean function f is a function from Z_2^n to Z_2
- The Walsh-Hadamard transform of f is defined by

$$S_f(u) = \sum_{v \in \mathbb{Z}_2^n} (-1)^{f(v)+u \cdot v}$$

Lemma

$$S_f(u) = 2^n \delta_{\vec{0},u} - 2\mathcal{H}_{f^{-1}(1)}((-1)^{u_1}, \ldots, (-1)^{u_n}).$$

Take $f^{-1}(1)$ to be a simplicial complex $\Delta \setminus \{0\}$

Walsh-Hadamard transform of a simplicial complex

Theorem (Chang-H, 2018)

Let Δ be a simplicial complex of Z_2^n and f a Boolean function in n variables with $f^{-1}(1) = \Delta^*$

Then

$$S_f(u) = 2^n \delta_{\vec{0},u} - 2 \sum_{\emptyset \neq S \subseteq \mathcal{F}} (-1)^{|S|+1} 2^{|\cap S|} \chi(u| \cap S),$$

where for X a subset of $\mathbb{Z}_2^n$, by $\chi(u|X)$ we mean a Boolean function in n-variable, and $\chi(u|X) = 1$ if and only if $u \cap X = \emptyset$.

Proof

1. $$\mathcal{H}_{\Delta}(x_1, \ldots, x_n) = \sum_{\emptyset \neq S \subseteq \mathcal{F}} (-1)^{|S|+1} \prod_{i \in \cap S} (1 + x_i)$$

2. $$S_f(u) = 2^n \delta_{\vec{0},u} - 2\mathcal{H}_{f^{-1}(1)}((-1)^{u_1}, \ldots, (-1)^{u_n}).$$

3. $$C_f = \{c_f(s,u) = (sf(x) + u \cdot x)_{x \in \mathbb{Z}_2^{n*}} : s \in \mathbb{Z}_2, u \in \mathbb{Z}_2^n\}$$

4. $$w_H\left(c_f(s,u)\right) = 2^{n-1} - \frac{1}{2} S_{sf}(u)$$

The weight distribution of C_f

1 Δ : a simplicial complex of Z_2^n generated by **one maximal element A**

2 Δ : a simplicial complex of Z_2^n generated by **two maximal element A and B**

$$C_f = \{c_f(s,u) = (sf(x) + u \cdot x)_{x \in \mathbb{Z}_2^{n*}} : s \in \mathbb{Z}_2, u \in \mathbb{Z}_2^n\}$$

where $f^{-1}(1) = \Delta^*$

One maximal element

Proposition
Let Δ be a simplicial complex of Z_2^n with **one maximal element A**
Let $f^{-1}(1) = \Delta^*$

$$C_f = \{c_f(s,u) = (sf(x) + u \cdot x)_{x \in \mathbb{Z}_2^{n*}} : s \in \mathbb{Z}_2, u \in \mathbb{Z}_2^n\}$$

Then the weight distribution of C_f is as follows:

$Weight$	$Frequency$
0	1
$2^{\lvert A\rvert} - 1$	1
$2^{n-1} - 1$	$2^{n-\lvert A\rvert}(2^{\lvert A\rvert} - 1)$
2^{n-1}	$2^n - 1$
$2^{n-1} + 2^{\lvert A\rvert} - 1$	$2^{n-\lvert A\rvert} - 1$

One maximal element

$Weight$	$Frequency$
0	1
$2^{\lvert A\rvert}-1$	1
$2^{n-1}-1$	$2^{n-\lvert A\rvert}(2^{\lvert A\rvert}-1)$
2^{n-1}	$2^{n}-1$
$2^{n-1}+2^{\lvert A\rvert}-1$	$2^{n-\lvert A\rvert}-1$

$|A| = n-1 : C_f = [2^n-1, n+1, 2^{n-1}-1]$: three-weight linear code (punctured first order Reed-Muller code)

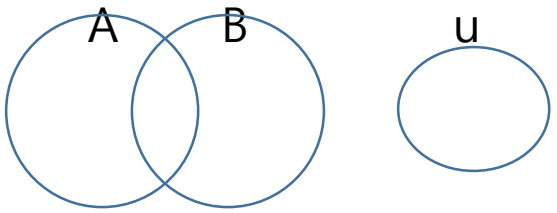
$|A| = n : C_f = [2^n-1, n+1, 2^{n-1}-1]$: two-weight linear code

Thus there exist non-equivalent optimal linear codes with parameters

$$[2^n-1, n+1, 2^{n-1}-1]$$

that attain Griesmer bound with equality

Two maximal elements



Let Δ be a simplicial complex of Z_2^n with **two maximal elements A and B**

$$C_f = \{c_f(s,u) = (sf(x) + u \cdot x)_{x \in \mathbb{Z}_2^{n*}} : s \in \mathbb{Z}_2, u \in \mathbb{Z}_2^n\}$$

$$S_{sf}(u) = 2^n \delta_{\vec{0},u} + \delta_{1,s}\left(-2^{|A|+1}\chi(u|A) - 2^{|B|+1}\chi(u|B) + 2^{|A\cap B|+1}\chi(u|A\cap B) + 2\right)$$

$$\chi(u|X) = 1 \text{ if and only if } u \cap X = \emptyset.$$

$$w_H\left(c_f(s,u)\right) = 2^{n-1} - \frac{1}{2}S_{sf}(u)$$

The weight distribution of C_f

Theorem (Chang-H, 2018)

Let Δ be a simplicial complex of Z_2^n generated by **two maximal elements A and B**
Let f be a Boolean function in n variables with $f^{-1}(1) = \Delta - \{0\}$

Then the weight distribution of C_f is given by

The weight distribution of C_f

i	A_i
0	1
$2^{\lvert A\rvert} + 2^{\lvert B\rvert} - 2^{\lvert A\cap B\rvert} - 1$	1
$2^{n-1} - 2^{\lvert A\cap B\rvert} - 1$	$2^{n-\lvert A\cup B\rvert}(2^{\lvert A\setminus B\rvert} - 1)(2^{\lvert B\setminus A\rvert} - 1)$
$2^{n-1} - 1$	$2^{n-\lvert A\cup B\rvert}(2^{\lvert A\cap B\rvert} - 1)2^{\lvert A\setminus B\rvert+\lvert B\setminus A\rvert}$
2^{n-1}	$2^n - 1$
$2^{n-1} + 2^{\lvert A\rvert} - 2^{\lvert A\cap B\rvert} - 1$	$2^{n-\lvert A\cup B\rvert}(2^{\lvert B\setminus A\rvert} - 1)$
$2^{n-1} + 2^{\lvert B\rvert} - 2^{\lvert A\cap B\rvert} - 1$	$2^{n-\lvert A\cup B\rvert}(2^{\lvert A\setminus B\rvert} - 1)$
$2^{n-1} + 2^{\lvert A\rvert} + 2^{\lvert B\rvert} - 2^{\lvert A\cap B\rvert} - 1$	$2^{n-\lvert A\cup B\rvert} - 1$

The weight distribution of C_f

Example

Let **n=10**, |A|=|B|=8 and $|A \cup B| = 10$
Then $|A \cap B| = 6$

i	A_i
$2^9 - 2^6 - 1$	$(2^2-1)^2 + 1 = 10$
$2^9 - 1$	$2^4(2^6-1) = 496$
2^9	$2^{10} - 1 = 1023$
$2^9 + 2^8 - 2^6 - 1$	$2(2^2 - 1) = 6$

The weight distribution of C_f

Example

Let **n=10**, |A|=|B|=5 and $|A \cup B| = 10$
Then $|A \cap B| = 0$

i	A_i
$2^6 - 12$	1
$2^9 - 2$	961
2^9	1023
$2^9 + 2^5 - 2$	62

Find a minimal linear code from C_f

Theorem (Chang-H, 2018)

Let $n \geq 4$
Let Δ be a simplicial complex of Z_2^n generated by **two maximal elements A and B**
Let f be a Boolean function in n variables with $f^{-1}(1) = \Delta - \{0\}$

Then C_f is minimal if and only if $A \cup B = [n]$ and $\max\{|A|, |B|\} \leq n - 2$

In this case, C_f does not satisfy A-B condition

Related works

Z. Heng, C. Ding, Z. Zhou, Minimal Linear Codes over Finite Fields, arXiv:1803.09988

Sporadic examples show that Ashikhmin-Barg's condition is not necessary for linear codes to be minimal. However, no infinite family of minimal linear codes with $\frac{d_{min}}{d_{max}} \leq (q-1)/q$ was found until the breakthrough in [7], where an infinite family of such binary codes was discovered.

J. Y. Hyun, H. K. Kim, M. Na, Non-projective optimal linear codes constructed from down set

Thank you for your attention