Griesmer bound의 등호를 만족하는 $[2^k-1+k,\ k,\ 2^{k-1}+1]$ 부호의 설계 방법

김정헌, 송홍엽
연세대학교 전기전자공학과

Construction of $[2^k-1+k,\ k,\ 2^{k-1}+1]$ code attaining Griesmer bound

Jeong-Heon Kim, Hong-Yeop Song
Department of Electrical and Electronics Engineering, Yonsei University

요약

모든 $[n,k,d]$ 이진 부호는 Griesmer bound $n \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil$를 만족해야 한다. 본 논문에서는 Griesmer bound의 등호를 만족하는 $[2^k-1+k,\ k,\ 2^{k-1}+1]$ 부호의 간단한 설계법을 소개하고 Helleseth 부호 관점에서 본 새로운 표현법을 소개한다.

Abstract

Any $[n,k,d]$ binary linear code must satisfy the Griesmer bound $n \geq \sum_{i=0}^{k-1} \lceil d/2^i \rceil$. Here, a simple construction of $[2^k-1+k,\ k,\ 2^{k-1}+1]$ codes which achieves the equality of the Griesmer bound is introduced and its another description in view of the codes of Helleseth is presented.

1. 소개의 글

이진 선형 $[n,k,d]$ 부호는 길이가 n, 차원이 k, 그리고 최소 거리가 d인 이진 선형 부호를 의미한다. 1960년에 Griesmer[1]는 모든 $[n,k,d]$ 부호가 (1)에 나타난 한계식을 만족함을 증명하였다. 여기에서 $\lceil x \rceil$는 x보다 크거나 같은 최소 정수이다.

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

편의상, $g(k,d)=\sum_{i=0}^{k-1} \lceil d/2^i \rceil$라 정의하자. 그러면, $n=g(k,d)$를 만족하는 $[n,k,d]$ 부

호는 Griesmer bound를 만족한다고 말한다. 주어진 k와 d에 대해서, n보다 더 작은 길이를 갖는 부호가 존재하지 않는다는 점에서 이 부호는 최적 부호이다.

1965년에 Solomon과 Stiffler[2]는 최적의 부호의 군을 제시하였다. 1974년 Belov[3]는 이 군의 일반화된 해석을 제공했고 또한 최적 부호의 또 다른 군의 생성 방법을 발표하였다. 이런 모든 부호들은 최소거리 $d \le 2^{k-1}$를 갖는다. 또한 Helleseth[4]는 $d \le 2^{k-1}$를 만족하는 다른 최적 부호가 없음을 증명하였다.

일반적으로, $d > 2^{k-1}$에 대해서도 최적 부호의 다양한 군이 Helleseth와 Van Tilborg[5][6]에 의해 알려졌다. 다음 장에서 $d = 2^{k-1}+1$을 갖는 최적 부호의 간단한 설계법을 소개하고 마지막으로 Helleseth의 관점에서 본 새로운 표현법을 제시한다.

2. Griesmer bound를 만족하는 $[2^k-1+k, k, 2^{k-1}+1]$ 부호

정리 1. 부호 C가 다음 생성 행렬을 갖는다고 하자.

$$C = [P_{2^k-1} \mid I_k] \tag{2}$$

여기에서 P_{2^k-1}는 $[2^{k-1}-1, 2^k-1-k]$ Hamming 부호의 패리티 검사 행렬이다. 그러면 C는 $[2^k-1+k, k, 2^{k-1}+1]$ 부호이고 Griesmer bound의 하한을 만족한다.

증명: 우선 C의 최소거리가 $2^{k-1}+1$임을 보이자. 어떤 C의 원소 $c(\neq 0)$에 대해서 $c = (h \mid m)$이다. 단, h는 $[2^{k-1}-1, 2^k-1-k]$ Hamming 부호의 dual 부호의 한 부호어이고 m은 어떤 정보 벡터이다. D의 0이 아닌 모든 부호어는 hamming 무게가 2^{k-1}이므로 c는 적어도 $2^{k-1}+1$을 무게로 갖는다. 따라서 C의 최소 거리는 $2^{k-1}+1$이다.

$$g(k,d) = \sum_{i=0}^{k-1} \lceil \frac{d}{2^i} \rceil = \sum_{i=0}^{k-1} \lceil \frac{2^{k-1}+1}{2^i} \rceil$$

$$= \sum_{i=0}^{k-1} (2^{k-1-i}+1)$$

$$= 2^k-1+k$$

여기서 C는 Griesmer bound의 하한을 만족함을 알 수 있다. □

일반적으로 모든 $[n, k, d]$ 부호로부터 단위 행렬과 원래의 생성 행렬을 결합시키므로서 새로운 선형 부호의 생성행렬을 만들 수 있다. 이 부호는 $n' = n+k, k' = k, d' = d+1$을 갖는다. 이 방법은 반복적으로 적용 가능하다. 이 방법을 해밍 부호의 dual 부호에 반복적으로 적용했을 때 n와 $g(k,d)$의 값들을 표 2에서 비교하였다. s가 증가함에 따라 n과 $g(k,d)$의 차이가 커짐이 관찰된다.

표 1. $3 \le k \le 13$에 대해서 C의 파라미터

n	k	d
10	3	5
19	4	9
36	5	17
69	6	33
134	7	65
263	8	129
520	9	257
1033	10	513
2058	11	1025
4107	12	2049
8204	13	4097

표 2. 덧붙여진 단위 행렬의 수에 따른 n의 비교.
여기에서 s는 덧붙여진 단위 행렬들의 수, 각각의 짝들의 첫 번째 요소는 n 이고, 두 번째 요소가 $n - g(n, k)$이다.

k	S					
	0	1	2	3	4	5
3	(7,0)	(10,0)	(13,3)	(16,5)	(19,6)	(22,8)
4	(15,0)	(19,0)	(23,4)	(27,7)	(31,9)	(35,12)
5	(31,0)	(36,0)	(41,5)	(46,9)	(51,12)	(56,16)
6	(63,,0)	(69,0)	(75,6)	(81,11)	(87,15)	(93,20)
7	(127,0)	(134,0)	(141,7)	(148,13)	(155,18)	(162,24)
8	(255,0)	(263,0)	(271,8)	(279,15)	(287,21)	(295,28)
9	(511,0)	(520,0)	(529,9)	(538,17)	(547,24)	(556,32)
10	(1023,0)	(1033,0)	(1043,10)	(1053,19)	(1063,27)	(1073,36)
11	(2047,0)	(2058,0)	(2069,11)	(2080,21)	(2091,30)	(2102,40)
12	(4095,0)	(4107,0)	(4119,12)	(4131,23)	(4143,33)	(4155,44)
13	(8191,0)	(8204,0)	(8217,13)	(8230,25)	(8243,36)	(8256,48)

3. 새로운 표현법

Helleseth[6]는 Griesmer bound를 만족하는 부호의 여러 알려진 군은 일반적인 형태로 표현될 수 있음을 증명하였다. 사실 본 논문의 부호 역시 같은 형태로 표현된다. S_k를 모든 가능한 이진 k-튜플이 열의 집합이 되는 행렬이라 하고 I_k를 차원이 k인 단위 행렬이라 하자. 그리고 $[A\backslash B]$를 B를 구성하는 모든 열을 A에서 제거한 행렬이라 하자. 그러면 식(2)에서 주어진 생성다항식은 $G=[S_k \mid S_k]\backslash G'$로 다시 쓸 수 있다(단 $G'=[S_k\backslash I_k]$이다). 여기서 G'은 C의 반-부호(anti-code)[7][8]의 생성 행렬이다. $\Phi(k,u)$는 U가 k차 벡터 공간의 u차 부분 공간에 있는 0이 아닌 벡터(열)로 이루어진 집합일 때 $U\in\Phi(k,u)$로 정의된다. 그리고 $\Psi(k,u)$는 V가 (3)의 행렬의 행 연산과 열 순열들로부터 얻어지는 열들의 집합이라 하면 $V\in\Psi(k,u)$에 의해 결정되는 것으로 정의한다.

$$\begin{bmatrix} 1\cdots1 & 0\cdots0 \\ U_1\backslash U_2 & U_2 \end{bmatrix} \tag{3}$$

$$(\ U_1\in\Phi(k-1,u_1),\ \ U_2\subset U_1\text{이고}\ \ U_2\in\Phi(k-1,u_2),\ \ u_2\le u_1=u\ )$$

Helleseth는 [6]에서 만약 부호 C의 반-부호 C'의 생성 다항식 G'가 $V_i\in\Psi(k,u_i)$, $k>u_1>\cdots>u_p\ge1$에서 $G'=[V_1 \mid V_2 \mid \cdots \mid V_p]$로 쓰여진다면, C는 Griesmer bound를 만족한다는 것을 보였다. 다음 정리는 2장에서 제시한 부호를 위의 형태로 표현할 수 있음을 증명한다. 이 정리에서 $U_k\in\Phi(k,k)$이다.

정리 2. $G'=[U_k\backslash I_k]$를 가정하자. 그러면 $V_i\in\Psi(k,k-i)$, $1\le i\le k-1$에 대하여 다음을 만족한다.

$$G'=[V_1 \mid V_2 \mid \cdots \mid V_{k-1}] \tag{4}$$

증명: k에 관한 수학적 귀납법으로 증명한다.

(1) $k=2$일 때 $[U_2\backslash I_2]=\begin{bmatrix}1&1&0\\1&0&1\end{bmatrix}\backslash\begin{bmatrix}1&0\\0&1\end{bmatrix}=\begin{bmatrix}1\\1\end{bmatrix}$는 오직 한 개의 열, $[1\ \ 1]^t$을 가진다. 따라서 $[U_2\backslash I_2]\in\Psi(2,1)$이다.

(2) 이제 $k>3$에서 생각하자. 그러면 귀납법의 가정에 의해서 다음 식을 얻는다.

$[U_{k-1}\backslash I_{k-1}]=[V_1' \mid \cdots \mid V_{k-2}']$, $V_i'\in\Psi(k-1,k-1-i)$, $1\le i\le k-2$

여기서 $V_{i+1}=\begin{bmatrix}0\cdots0\\V_i'\end{bmatrix}$, $1\le i<k-2$, $V_1=\begin{bmatrix}1\cdots1\\U_{k-1}\end{bmatrix}$라 놓으면 $V_{i+1}\in\Psi(k,k-1-i)$,

$V_i \in \Psi(k, k-1)$이다. 따라서

$$U_k = \begin{bmatrix} 1\cdots1 & 1 & 0\cdots0 \\ & 0 & \\ U_{k-1} & \vdots & U_{k-1} \\ & 0 & \end{bmatrix}$$

이므로, 다음 식이 성립한다.

$$[V_1 \mid \cdots \mid V_{k-1}] = \begin{bmatrix} 1\cdots1 & 0\cdots0 \\ U_{k-1} & U_{k-1} \backslash I_{k-1} \end{bmatrix} = [U_k \backslash I_k] = G' \quad \square$$

2장에서 제시한 코드 C의 반-부호의 생성 행렬 G'가 $G' = [S_k \backslash I_k]$로 표현됨을 상기하자. $S_k \in \Phi(k, k)$이므로 G'는 식(4)에서 나타난 형태로 쓸 수 있다.

참고문헌

[1] J. H. Griesmer, "A bound for error-correcting codes," IBM J. Res. Develop., vol.4, pp.532-542, 1960.

[2] G. Solomon and J. J. Stiffler, "Algebraically punctured cyclic codes," Inform. Contr., vol.8, pp.170-179, 1965.

[3] V. I. Belov, "A conjecture on the Griesmer bound," Optimization Methods and Their Applications, pp.100-106, 1974.

[4] Tor Helleseth, "A characterization of codes meeting the Griesmer bound," Inform. Contr., vol.50, pp.128-159, Aug. 1981.

[5] T. Helleseth and H/C. A van Tilborg, "A new class of codes meeting the Griesmer bound," IEEE trans. Inform. Theory, vol. IT-27, pp.548-555, Sept. 1981.

[6] Tor Helleseth, "New constructions of codes meeting the Griesmer bound," IEEE trans. Inform. Theory, vol. IT, no.3, pp434-439, May. 1983.

[7] P. G. Farrell, "Linear binary anticodes," Electron. Lett., vol.6, pp.419-421, June. 1970.

[8] P. G. Farrell, "An introduction to anticodes," in Algebraic Coding Theory and Applications. Springer Verlag, New York, 1979.