차분행렬을 리용한 최량동등기호무게부호의 구성방법

김 성 철

경애하는 **김정은**동지께서는 다음과 같이 말씀하시였다.

《이미 일정한 토대가 있고 전망이 확고한 연구대상들에 힘을 넣어 세계패권을 쥐며 그 성과를 확대하는 방법으로 과학기술을 빨리 발전시켜야 합니다.》

동등기호무게부호는 전력선통신에서 통신부호의 정확도를 높이기 위하여 제안되였으며 그 구성법에 대해서도 일정한 연구가 진행되였다.[1－3]

론문에서는 차분행렬을 리용하여 현재까지 존재성과 구성법이 밝혀지지 않은 파라메터들을 가진 동등기호무게부호를 구성한다.

k를 정의옹근수라고 하자. k를 모듈로 하는 옹근수모임의 잉여환 $\{0, 1, \cdots, k-1\}$을 $\mathbf{Z}_k$로 표시하며 첫 k개의 자연수들의 모임을 I_k로 표시하자.

부호단어길이가 n이고 부호단어개수가 M이며 최소해밍거리가 d인 $q-$진부호 $\mathcal{C}\subseteq Q^n$을 $(n, M, d; q)-$부호라고 말한다. $(n, M, d; q)-$부호 $\mathcal{C}$에 대하여 그것의 부호단어들이 모두 동등기호무게를 가진다면 동등기호무게부호라고 부르고 $(n, M, d; q)-$ESWC라고 표시한다.

$(n, M, d; q)-$ESWC $\mathcal{C}\subseteq Q^n$은 협대역잡음오유를 $c(\mathcal{C})-1$개까지 정정할수 있다.[2]

여기서 $c(\mathcal{C})=\min\{e: E_{\mathcal{C}}(e)\geq d\}$이고 $E_{\mathcal{C}}(e)=\max\limits_{\substack{T\subset Q\\|T|=e}}\max\limits_{c\in\mathcal{C}}\left\{\sum\limits_{x\in T}w_x(c)\right\}$이다.

n, d와 q가 주어졌을 때 $(n, M, d; q)-$ESWC의 최대크기 M을 $A_q^{esw}(n, d)$로 표시한다. 크기가 $M=A_q^{esw}(n, d)$인 $(n, M, d; q)-$ESWC는 최량이라고 말한다.

부호크기의 웃한계로 알려진 뽈로뜨낀한계를 ESWC의 최량성을 측정하는 기준으로 리용할수 있다.

정리 1 [2] $d\leq n$과 $qd>n(q-1)$을 만족시키는 임의의 n, q, d에 대하여 관계식 $A_q^{esw}(n, d)\leq qd/(qd-(q-1)n)$가 성립된다.

동등기호무게부호와 일반화된 균형적시합배치사이에는 밀접한 관계가 있다.

정리 2[2] GBTD(k, m)이 존재할 때 그리고 그때에만 뽈로뜨낀한계에 도달하는 최량 $(n, M, d; q)-$ESWC가 존재한다. 여기서 $n=km-1$, $M=km$, $d=k(m-1)$, $q=m$이다.

이 정리로부터 q가 홀씨수의 제곱인 경우 차분행렬을 리용하여 GBTD(q, q)를 구성하고 이것을 리용하여 동등기호무게부호를 구성할수 있다.[2]

그러나 기술적제한성으로 하여 q가 2의 제곱인 경우에는 구성법도, 존재성도 밝히지 못하였다.

론문에서는 차분행렬의 존재성이 아직까지 미해결로 남아있는 경우인 $n=2^k$, $k\geq 2$인 경우 $(n^2-1, n^2, n(n-1); n)-$ESWC를 차분행렬을 리용하여 구성한다.

보조정리 1 위수가 k 인 더하기군우에서의 균일한 $(k,\ k,\ k-1)-\mathrm{DM}$ 이 존재하면 최량 $(n,\ M,\ d;\ q)-\mathrm{ESWC}$ 가 존재한다. 여기서 $n=k^2-1,\ M=k^2,\ d=k(k-1),\ q=k$ 이다.

증명 $G=\{g_0=0,\ g_1,\ \cdots,\ g_{k-1}\}$ 이라고 하고 $D=(d_{ij})\ (i\in\mathbf{Z}_k,\ j\in I_{(k-1)k})$ 를 G 우에서의 균일한 $(k,\ k,\ k-1)-\mathrm{DM}$ 이라고 하면 다음과 같이 부호단어들을 구성할수 있다.

먼저 D 의 매행 $(d_{i,\,1},\ d_{i,\,2},\ \cdots,\ d_{i,\,k(k-1)})$ 에 대하여 G 우에서의 $k\times k(k-1)$ 형행렬을

$$M(i)=\begin{pmatrix} d_{i,\,1}+g_0 & d_{i,\,2}+g_0 & \cdots & d_{i,\,k(k-1)}+g_0 \\ d_{i,\,1}+g_1 & d_{i,\,2}+g_1 & \cdots & d_{i,\,k(k-1)}+g_1 \\ \vdots & \vdots & \ddots & \vdots \\ d_{i,\,1}+g_{k-1} & d_{i,\,2}+g_{k-1} & \cdots & d_{i,\,k(k-1)}+g_{k-1} \end{pmatrix},\ i\in\mathbf{Z}_k$$

와 같이 구성한다.

모든 $i\in\mathbf{Z}_k$ 에 대하여 $M(i)$ 의 매렬들은 G 의 모든 원소들을 꼭 한번씩 포함하며 매 행들은 G 의 모든 원소들을 꼭 $k-1$ 번씩 포함한다. 그리고 $M(i)$ 의 서로 다른 두 행은 어느 성분도 같지 않다. 이 k 개의 배렬 $M(j)\ (j\in\mathbf{Z}_k)$ 들을 덧붙여서 다음과 같이 G 우에서의 $k^2\times k(k-1)$ 형행렬 N_1 을 구성하고 G 우에서의 $k^2\times(k-1)$ 형배렬 N_2 를 구성한다.

$$\boldsymbol{a}_1=\begin{pmatrix} M(0) \\ M(1) \\ \vdots \\ M(k-1) \end{pmatrix},\ \boldsymbol{a}_2=\begin{pmatrix} \bar{g}_0 & \bar{g}_1 & \cdots & \bar{g}_{k-2} \\ \bar{g}_1 & \bar{g}_2 & \cdots & \bar{g}_{k-1} \\ \vdots & \vdots & \ddots & \vdots \\ \bar{g}_{k-1} & \bar{g}_0 & \cdots & \bar{g}_{k-3} \end{pmatrix}$$

여기서 $\bar{g}_i$ 는 성분들이 모두 g_i 인 $k\times 1$ 형렬벡토르를 나타낸다.

끝으로 N_1 과 N_2 를 덧붙이면 G 우에서의 $k^2\times(k^2-1)$ 형행렬 $(N_1\ N_2)$ 를 얻는다.

N_2 의 k^2 개의 행벡토르들을 차례로 k 개씩 그룹을 지으면 같은 그룹에 속하는 벡토르들은 $k-1$ 개의 성분들이 모두 같으며 서로 다른 그룹에 속하는 두 벡토르들은 같은 성분이 하나도 없다. 행렬 $(N_1\ N_2)$ 의 k^2 개의 매 행들을 부호단어로 하는 부호는 G 우에서의 $(k^2-1,\ k^2,\ k(k-1);k)-\mathrm{ESWC}$ 이다. 또한 크기 k^2 은 뽈로뜨낀한계에 도달한다.(증명끝)

보조정리 2 $n=2^k,\ k\geq 2$ 일 때 균일한 $(n,\ n,\ n-1)-\mathrm{DM}$ 이 존재한다.

증명 G 를 유한체 $\mathbf{F}_n=\mathbf{Z}_2[x]/(g(x))$ 의 더하기군으로 취한다. 여기서 $g(x)\in\mathbf{Z}_2[x]$ 는 k 차기약다항식이다.

$\mathbf{F}_n$ 의 원소들은 $\mathbf{Z}_2[x]$ 의 차수가 기껏 $k-1$ 인 다항식으로 표현된다. 편리상 $\mathbf{F}_n$ 의 원소 $0,\ 1,\ x,\ x+1,\ \cdots,\ x^{k-1}+x^{k-2}+\cdots+x+1$ 들을 각각 $a_0,\ a_1,\ a_2,\ a_3,\ \cdots,\ a_{n-1}$ 로 표시한다.

$\mathbf{F}_n$ 우에서 n 차행렬 $D_1,\ D_2,\ \cdots,\ D_{n-1}$ 을 다음과 같이 구성한다.

$$D_i=\begin{pmatrix} a_1a_0 & a_1a_1 & a_1a_2 & \cdots & a_1a_{n-1} \\ a_2a_0 & a_2a_1 & a_2a_2 & \cdots & a_2a_{n-1} \\ a_3a_0 & a_3a_1 & a_3a_2 & \cdots & a_3a_{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1}a_0 & a_{n-1}a_1 & a_{n-1}a_2 & \cdots & a_{n-1}a_{n-1} \\ a_i & a_i & a_i & \cdots & a_i \end{pmatrix},\ i=\overline{1,\ n-1}$$

D_i 의 행들은 $\{1, 2, 3, \cdots, n\}$ 의 원소들로, 렬들은 $\{a_0, a_1, a_2, \cdots, a_{n-1}\}$ 의 원소들로 번호를 붙인다.

매 D_i 에 대하여 D_i 의 임의의 서로 다른 두 행의 차가 $\mathbf{F}_n$ 의 원소들을 꼭 한번씩 포함한다는것 즉 차분행렬이라는것은 쉽게 알수 있다.

따라서 행렬 $D^{*1} = (D_1 | D_2 | D_3 | \cdots | D_{n-1})$ 도 차분행렬이다.

그런데 D^{*1} 에서 첫 $n-1$ 개의 행들에는 모든 원소들이 다 $n-1$ 번씩 포함되지만 마지막행에는 $a_1, a_2, a_3, \cdots, a_{n-1}$ 들이 각각 n 번씩 포함되며 $a_0(=0)$ 은 포함되지 않는다. 즉 균일하지 않다.

D^{*1} 을 균일하게 변경시키기 위하여 먼저 매 D_i 의 마지막행들에서 각각 하나의 원소씩을 $a_0(=0)$ 으로 바꾼다.

$i = \overline{1,\ n-1}$ 에 대하여 매 D_i 에서 마지막행의 j_i 렬의 원소들을 a_0 으로 바꾸어 얻은 행렬을 D^{*2} 이라고 하자. 이때 D^{*1} 과 D^{*2} 에서 바꾼 원소를 포함하는 렬들만을 추려서 보면 다음과 같다.(표 1, 2)

표 1. 교체전의 렬들

$a_1 j_1$	$a_1 j_2$	$\cdots$	$a_1 j_{n-1}$
$a_2 j_1$	$a_2 j_2$	$\cdots$	$a_2 j_{n-1}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$a_{n-1} j_1$	$a_{n-1} j_2$	$\cdots$	$a_{n-1} j_{n-1}$
a_1	a_2	$\cdots$	a_{n-1}

표 2. 교체후의 렬들

$a_1 j_1$	$a_1 j_2$	$\cdots$	$a_1 j_{n-1}$
$a_2 j_1$	$a_2 j_2$	$\cdots$	$a_2 j_{n-1}$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$a_{n-1} j_1$	$a_{n-1} j_2$	$\cdots$	$a_{n-1} j_{n-1}$
a_0	a_0	$\cdots$	a_0

D^{*1} 에서 임의의 서로 다른 두 행의 차는 $\mathbf{F}_n$ 의 원소들을 꼭 $n-1$ 번씩 포함한다.

우리는 D^{*2} 에서 첫행과 마지막행의 차가 $\mathbf{F}_n$ 의 원소들을 꼭 $n-1$ 번씩 포함하도록 한다.

첫행과 마지막행의 차는 D^{*1} 에서는 $(j_1 + a_1,\ j_2 + a_2,\ \cdots,\ j_{n-1} + a_{n-1})$ 이고 D^{*2} 에서는 $(j_1,\ j_2,\ \cdots,\ j_{n-1})$ 이다. $a_1 = 1,\ a_0 = 0$ 이고 G 에서 $+$ 와 $-$ 는 동등하다.

$\{j_1 + a_1,\ j_2 + a_2,\ \cdots,\ j_{n-1} + a_{n-1}\} = \{j_1,\ j_2,\ \cdots,\ j_{n-1}\}$ 이도록 하기 위하여 $j_i,\ i = \overline{1,\ n-1}$ 들을

$$\begin{cases} j_1 + a_1 = j_2 \\ j_2 + a_2 = j_3 \\ \quad \cdots \\ j_{n-2} + a_{n-2} = j_{n-1} \\ j_{n-1} + a_{n-1} = j_1 \end{cases}$$

과 같은 $\mathbf{F}_n$ 우의 련립1차방정식의 풀이로 놓는다.

이 련립방정식을 다시 쓰면 $\begin{cases} j_1 + j_2 = a_1 \\ j_2 + j_3 = a_2 \\ \quad \cdots \\ j_{n-2} + j_{n-1} = a_{n-2} \\ j_{n-1} + j_1 = a_{n-1} \end{cases}$ 인데 결수행렬과 확대행렬은 다음과 같다.

$$\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 1 & \cdots & 0 & 0 \\ & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 & 0 & a_1 \\ 0 & 1 & 1 & \cdots & 0 & 0 & a_2 \\ & & & \cdots & & & \\ 0 & 0 & 0 & \cdots & 1 & 1 & a_{n-2} \\ 1 & 0 & 0 & \cdots & 0 & 1 & a_{n-1} \end{pmatrix}$$

이 행렬들은 둘 다 모든 행벡토르들의 합이 0벡토르이며 결수행렬의 임의의 $n-2$개 행은 1차독립이다. 그러므로 결수행렬과 확대행렬의 위수는 $n-2$로서 같으며 련립1차방정식은 풀이를 가진다. 풀이는 다음과 같다.

$$(j_1,\ j_2,\ \cdots,\ j_{n-1}) \in \{(c,\ c+a_1,\ c+a_1+a_2,\ \cdots,\ c+a_1+a_2+\cdots+a_{n-2}) : c \in \mathbf{F}_n\}$$

그러므로 첫행과 마지막행의 차에는 $\mathbf{F}_n$의 매 원소들이 꼭 $n-1$번씩 포함되면서 마지막행에도 $\mathbf{F}_n$의 매 원소들이 꼭 $n-1$번씩 포함되도록 D^{*2}를 구성할수 있다.

이렇게 구성한 D^{*2}가 $D^{*2} = (D_1' | D_2' | D_3' | \cdots | D_{n-1}')$과 같다고 하자.

새롭게 제기되는 문제는 $2 \sim (n-1)$ 행들과 마지막행의 차가 균일성이 파괴되는것이다. 이 문제를 해결하기 위하여 $D_i',\ i = \overline{1,\ n-1}$의 $2 \sim (n-1)$ 행들에 각각 어떤 상수를 더하겠다. 이러한 더하기연산은 $D_i',\ i = \overline{1,\ n-1}$의 $1 \sim (n-1)$ 행들중 임의의 2개의 행의 차의 균일성에는 영향을 주지 못한다. 그러므로 $D_i',\ i = \overline{1,\ n-1}$의 $1 \sim (n-1)$ 행들의 j_i 렬의 원소들이 일치하도록 $D_i',\ i = \overline{1,\ n-1}$의 $2 \sim (n-1)$ 행들에 각각 적당한 상수(정확하게는 $j_i + a_r j_i$, 여기서 $r = \overline{2,\ n-1}$은 행번호)를 더하면 이 문제가 해결된다는것을 곧 알수 있다.

이렇게 얻은 행렬 D^{*3}은 균일한 $(n,\ n,\ n-1)-\mathrm{DM}$ 이다.(증명끝)

보조정리 1, 2로부터 다음의 결과가 곧 나온다.

정리 3 $n = 2^k,\ k \geq 2$일 때 최량$(n^2-1,\ n^2,\ n(n-1); n)-\mathrm{ESWC}$가 존재한다.

참 고 문 헌

[1] **김일성**종합대학학보 수학, 65, 3, 24, 주체108(2019).

[2] P. P. Dai et al.; Des. Codes Cryptogr., 74, 15, 2015.

[3] L. A. Bassalygo et al.; Problems of Information Transmission, 50, 4, 2014.

주체110(2021)년 3월 5일 원고접수

A Method to Construct Optimal Equitable Symbol Weight Codes Using Difference Matrices

Kim Song Chol

In this paper, optimal equitable symbol weight codes meeting the Plotkin bound are constructed via difference matrices.

Keywords: generalized balanced tournament design(GBTD), difference matrix, equitable symbol weight code