김일성종합대학학보 주체108(2019)년
수 학 제65권 제4호

n이 2의 제곱일 때 일반화된 균형적시합배치 GBTD$(n,\ n)$의 구성

김성철, 김성남

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《나라의 과학기술을 세계적수준에 올려세우자면 발전된 과학기술을 받아들이는것과 함께 새로운 과학기술분야를 개척하고 그 성과를 인민경제에 적극 받아들여야 합니다.》(《**김정일**선집》 증보판 제11권 138~139페지)

GBTD$(k,\ m)$은 다른 조합적배치의 구성에서도 리용되며 동등기호무게부호의 구성을 비롯하여 부호리론에서 자주 리용되는것으로 하여 그것의 존재성과 구성법[1, 2]에 대한 연구가 많이 진행되였다. GBTD의 구성방법들을 보면 여러가지 보조적인 배치를 리용하는 방법, 차분행렬을 리용하여 구성하는 방법, GBTD$(k,\ k)$와 동등한 k^2차행렬의 구성에 의한 방법 등이 있다.

론문에서는 아직까지 미해결로 남아있는 경우인 $n=2^k,\ k\geq 2$인 경우 GBTD$(n,\ n)$을 차분행렬을 리용하여 구성한다.

우리는 론문에서 다음의 표기들을 리용한다.

$\mathbf{Z}_k=\{0,\ 1,\ \cdots,\ k-1\}$은 k를 모듈로 하는 옹근수모임의 잉여환이다.

$\mathbf{F}_n$은 원소수가 n인 유한체이다.

우리의 결과는 다음의 두가지 보조정리에 기초하고있다.

보조정리 1[2] 위수가 k인 가법군우에서의 균일한 $(n,\ n,\ n-1)-\mathrm{DM}$이 존재하면 $G\times\mathbf{Z}_k$우에서의 GBTD$(n,\ n)$이 존재한다.

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

증명 G를 유한체 $\mathbf{T}_n=\mathbf{Z}_2[x]/(g(x))$의 가법군으로 취한다. 여기서 $g(x)\in\mathbf{Z}_2[x]$는 k차 기약다항식이고 $\mathbf{F}_n$의 원소들은 $\mathbf{Z}_2[x]$의 차수가 기껏 $k-1$인 다항식으로 표현되며 $\mathbf{F}_n$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 n차행렬 $D_1,\ D_2,\ \cdots,\ D_{n-1}$을 다음과 같이 구성한다.

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

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

때문에 행렬 $D^{*1}=(D_1|D_2|D_3|\cdots|D_{n-1})$ 역시 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 n번씩 포함되며 $a_0(=0)$은 포함되지 않는다. 즉 균일하지 않다.

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

$i=\overline{1,\ n-1}$에 대하여 매 D_i에서 마지막행의 j_i렬의 원소들을 a_0으로 교체하여 얻은 행렬을 D^{*2}라고 하자.

이때 D^{*1}과 D^{*2}에서 바꾼 원소를 포함하는 렬들만을 추려서 보면 다음과 같다.(표 1, 2)

표 1. 교체전의 원소들

a_1j_1	a_1j_2	$\cdots$	a_1j_{n-1}
a_2j_1	a_2j_2	$\cdots$	a_2j_{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 원소들

a_1j_1	a_1j_2	$\cdots$	a_1j_{n-1}
a_2j_1	a_2j_2	$\cdots$	a_2j_{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 G에서 $+$와 $-$는 동등하다는것을 주의해둔다.

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

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

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

이 방정식을 다시 쓰면

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

인데 결수행렬과 확대행렬은 다음과 같다.

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

이 행렬들은 둘 다 모든 행벡토르들의 합이 0벡토르이며 결수행렬의 임의의 $n-2$개 행은 1차독립이다. 그러므로 결수행렬과 확대행렬의 위수는 $n-2$로서 같고 련립1차방정식은 풀이를 가지며 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 차가 $\mathbf{F}_n$ 의 원소들을 꼭 $n-1$번씩 포함하면서 마지막행이 $\mathbf{F}_n$ 의 원소들을 꼭 $n-1$번씩 포함하도록 D^{*2} 를 구성할수 있다.

이렇게 구성한 D^{*2} 가 $D^{*2}=(D'_1 \mid D'_2 \mid D'_3 \mid \cdots \mid D'_{n-1})$ 과 같다고 하자.

새롭게 제기되는 문제는 $2 \sim (n-1)$ 행들과 마지막행의 차들의 균일성이 파괴되는것이다.

이 문제를 해결하기 위하여 $D'_i,\ i=\overline{1,\ n-1}$ 의 $2 \sim (n-1)$ 행들에 각각 어떤 상수를 더한다. 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 $j_i + a_r j_i$, $r=\overline{2,\ n-1}$ 은 행번호)를 더하면 이 문제가 해결된다는것을 알수 있다.

이렇게 얻은 행렬 D^{*3} 은 균일한 $(8,\ 8,\ 7)-\mathrm{DM}$ 이다.(증명끝)

보조정리 1, 2로부터 다음의 결과가 곧 나온다.

정리 $n=2^k,\ k \ge 2$ 일 때 $\mathrm{GBTD}(n,\ n)$ 이 존재한다.

참 고 문 헌

[1] C. J. Colbourn et al.; The CRC Handbook of Combinatorial Designs, CRC Press, 72～336, 2007.

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

주체108(2019)년 6월 10일 원고접수

Construction of Generalized Balanced Tournament Designs GBTD(n, n) when n is 2's Power

Kim Song Chol, Kim Song Nam

We construct the generalized balanced tournament designs $\mathrm{GBTD}(n,\ n)$ when $n=2^k,\ k \ge 2$, using difference matrices.

Key word: difference matrix