김일성종합대학학보 JOURNAL OF **KIM IL SUNG** UNIVERSITY
(자연과학) (NATURAL SCIENCE)
주체106(2017)년 제63권 제1호 Vol. 63 No. 1 JUCHE106(2017).

유한체를 리용한 일반화된 균형적시합배치의 한가지 구성법

김 성 철

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《수학, 물리학, 화학, 생물학과 같은 기초과학부문에서 과학기술발전의 원리적, 방법론적기초를 다져나가면서 세계적인 연구성과들을 내놓아야 합니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 40폐지)

일반화된 균형적시합배치 GBTD$(k,\ m)$은 블로크들을 두가지 조건 즉 점모임의 모든 원소는 매 렬의 꼭 1개 블로크에 포함되며 매 행의 기껏 k개 블로크에 포함된다는 조건이 만족되도록 $m\times(km-1)$형행렬로 배렬할수 있는 $(km,\ k,\ k-1)-$BIBD이다.

선행연구[1－5]에서는 $k=2,\ 3,\ 4$인 경우 GBTD$(k,\ m)$의 존재성을 밝혔으며 GBTD$(k,\ k)$와 동등한 k^2차행렬을 도입하여 $p>2$가 씨수일 때 GBTD$(p,\ p)$를 구성하였다.

론문에서는 GBTD$(p,\ p)$를 리용하여 $p>2$가 홀씨수, $n\geq 2$일 때 GBTD$(p^n,\ p^n)$을 구성하였다.

정의[3] V를 원소(점이라고 부른다.)가 v개인 모임, B를 V의 어떤 $k-$부분모임(블로크)들의 모임이라고 하자.

V의 임의의 서로 다른 두 원소들이 B의 꼭 λ개의 블로크들에 같이 포함되면 순서붙은 쌍 $(V,\ B)$를 $(v,\ k,\ \lambda)-$균형적불완전블로크배치 또는 $(v,\ k,\ \lambda)-$BIBD라고 부른다.

$(v,\ k,\ \lambda)-$BIBD는 블로크를 $\lambda v(v-1)/k(k-1)$개 가진다. 즉 $(km,\ k,\ k-1)-$BIBD는 $m(km-1)$개의 블로크를 가진다.

보조정리 1[6] GBTD$(k,\ m)$의 모든 점은 $m-1$개 행들에는 k번 포함되며 나머지 한 행에는 $k-1$번 포함된다.

R를 GBTD$(k,\ m)$이라고 하면 R의 i행에서 꼭 $k-1$개 블로크에 포함되는 점을 i행의 부족점이라고 부른다.

R의 매 행이 부족점을 k개 가진다는것을 쉽게 알수 있다. 이 k개의 부족점들로 이루어진 $k-$원소조를 i행의 부족$k-$원소조라고 부른다.

보조정리 2[4] GBTD$(k,\ m)$의 부족$k-$원소조들은 점모임의 분할을 이룬다.

모든 정의옹근수 $m\neq 2$에 대하여 GBTD$(2,\ m)$, GBTD$(3,\ m)$이 존재하며 GBTD$(k,\ 2)$는 존재하지 않는다.[3]

또한 $m\geq 5,\ \ m\notin\{28,\ 32,\ 33,\ 34,\ 37,\ 38,\ 39,\ 44\}$일 때 GBTD$(4,\ m)$이 존재한다.[4]

선행연구[1, 2]에서는 GBTD$(k,\ k)$와 동등한 k^2차행렬을 도입하여 $p>2$가 씨수일 때 GBTD$(p,\ p)$를 구성하였다.

1. GBTD(k, k)와 동등한 k^2차행렬

여기서는 GBTD(k, k)와 동등한 $Z_k = \{0, 1, 2, \cdots, k-1\}$우에서의 k^2차행렬을 도입한다.

어떤 GBTD(k, k), $R = (r_{ij})$ (R의 행들은 Z_k의 원소들로 번호를 붙이고 렬들은 $\{1, 2, \cdots, k^2-1\}$의 원소들로 번호를 붙이자.)가 하나 있다고 하고 이 R에 대응되는 Z_k우에서의 k^2차행렬 $M' = (m_{ij})$를 구성하자.

R의 점모임 V를 $\{1, 2, \cdots, k^2\}$이라고 하면 R의 k^2-1개의 매 렬에는 V의 매 점이 꼭 한번씩 포함되여있다.

$1 \le i \le k^2-1$, $1 \le j \le k^2$인 i, j에 대하여 j가 블로크 r_{ki}에 포함되여있다면 $m_{i+1,\ j} = k$로 놓는다.

보조정리로부터 M'의 모든 j렬$(1 \le j \le k^2)$에서 첫번째 행원소를 제외한 나머지원소들중에는 Z_k의 꼭 1개 원소(d_j라고 표시)가 꼭 $k-1$번 포함되며 나머지원소들은 꼭 k번씩 포함된다.

m_{1j}를 d_j로 놓는다. 분명히 Z_k의 임의의 원소 i에 대하여 M'의 첫번째 행에서 i가 포함되는 렬번호들의 모임은 R의 i행의 부족k－원소조이다.

실례 1 GBTD(3, 3) $R=$

129	349	569	145	357	178	238	267	*468*
357	167	138	236	468	245	749	589	*129*
468	258	247	789	129	369	165	134	*357*

에 대응되는 행렬 M'는 다음과 같다.(사선으로 쓴 부분은 매 행의 부족3–원소조이다.)

$M'=$

1	1	2	0	2	0	2	0	1
0	0	1	2	1	2	1	2	0
1	2	0	0	2	1	1	2	0
1	2	1	2	0	0	2	1	0
0	1	1	0	0	1	2	2	2
2	2	0	1	0	1	0	1	2
0	1	2	1	1	2	0	0	2
2	0	0	1	2	2	1	0	1
2	0	2	2	1	0	0	1	1

어떤 GBTD(k, k)가 주어졌을 때 세가지 연산 즉 행과 행의 자리바꾸기, 렬과 렬의 자리바꾸기, 점모임우에서의 치환을 적용하여 동등한 GBTD(k, k)를 얻을수 있다.

이 연산들은 Z_k우에서의 행렬의 세가지 연산 즉 기초모임 Z_k우에서의 치환, 첫번째 행을 제외한 나머지행들중에서 두 행의 자리바꾸기, 렬과 렬의 자리바꾸기와 각각 대응된다.

M'에서 렬과 렬의 자리바꾸기를 몇번 실시하여 첫 행의 첫 k개 원소들이 0, 다음 k개 원소들이 1, 이런 식으로 계속하여 마지막 k개 원소들이 $k-1$인 행렬 M을 얻을수 있다.

행렬 M의 첫 k개 렬을 V_0, 다음 k개 렬을 V_1, 마지막 k개 렬을 V_{k-1}이라고 표시

하자. 즉 $M=(V_0,\ V_1,\cdots,\ V_{k-1})$ 이라고 표시하자.

행렬 M 의 구성과정으로부터 M 이 다음의 성질을 가진다는것을 알수 있다.

① M 의 매 행, 매 렬은 Z_k 의 모든 원소들을 꼭 k 번씩 포함한다.

② 임의의 $i\ (0\le i\le k-1)$ 에 대하여 V_i 에 속하는 서로 다른 두 렬은 꼭 k 개 행에서 같은 원소를 포함한다.

③ 임의의 $i,\ j\ (0\le i<j\le k-1)$ 에 대하여 $V_i,\ V_j$ 에 각각 속하는 두 렬은 꼭 $k-1$ 개 행에서 같은 원소를 포함한다.

실례 2 실례 1의 행렬 M' 의 임의의 두 렬은 첫 행을 제외한 나머지행들중 꼭 2개 행에서 같은 원소를 포함한다. 례하면 첫 렬과 둘째 렬은 2째 행과 6째 행에서, 넷째 렬과 다섯째 렬은 5째 행과 7째 행에서 같은 원소를 포함한다. M' 의 매 행, 매 렬은 0, 1, 2를 각각 3번씩 포함한다.

우의 성질들이 만족되는 행렬로부터 GBTD$(k,\ k)$ 를 거꾸로 얻을수 있다는것을 쉽게 알수 있다.

2. GBTD$(p^n,\ p^n)$ 의 구성

여기서는 p 는 홀씨수, n 은 2이상의 옹근수일 때 GBTD$(p^n,\ p^n)$ 을 구성한다.

$q=p^n$ 이라고 하자.

앞에서와 같은 성질을 가진 체 $\mathbf{F}_q(=\mathbf{F}_{p^n})$ 우에서의 $q^2(=p^{2n})$ 차행렬 M_q 를 구성하자.

우리는 체 $\mathbf{F}_q$ 의 원소들에 대하여 다음의 표기법을 리용한다.

체 $\mathbf{F}_q$ 는 씨체 F_p 의 n 차대수적단순확대체이다.

만일 f 가 $\mathbf{F}_p[x]$ 의 n 차기약다항식이면 이 다항식의 임의의 뿌리 α 는 체 $\mathbf{F}_q$ 에 속하며 $\mathbf{F}_q=\mathbf{F}_p(\alpha)$ 이다. 이때 $\mathbf{F}_q$ 에서 $f(\alpha)=0$ 이며 $\mathbf{F}_q$ 의 원소들은

$$a_{n-1}\alpha^{n-1}+a_{n-2}\alpha^{n-2}+a_{n-3}\alpha^{n-3}+\cdots+a_1\alpha+a_0$$

모양으로 표시할수 있다. 여기서 $a_0,\ a_1,\ a_2,\cdots,\ a_{n-1}\in F_p$ 이다.

$\mathbf{F}_q$ 의 원소 $a_{n-1}\alpha^{n-1}+a_{n-2}\alpha^{n-2}+a_{n-3}\alpha^{n-3}+\cdots+a_1\alpha+a_0$ 을 p 진표기법을 리용하여 간단히 $(a_{n-1}a_{n-2}a_{n-3}\cdots a_1a_0)_p$ 로 표시한다.

또한 $\mathbf{F}_q$ 의 원소들을 $\{(0)_q,\ (1)_q,\ (2)_q,\cdots,\ (q-1)_q\}$ 로도 표시하는데 이때 원소 $(a)_q$ 는 수 a 의 p 진표기에 대응되는 원소로 생각한다.

몇가지 기호를 약속하자.

행렬 M_q 의 첫 q 개 행을 H^* 이라고 하고 나머지 q^2-q 개 행들을 차례로 $q-1$ 개씩 묶어서 각각 $H_{(0)_q},\ H_{(1)_q},\ H_{(2)_q},\cdots,\ H_{(q-1)_q}$ 라고 하자.

행렬 M_q 의 렬들을 차례로 q 개씩 묶어서 각각 $V_{(0)_q},\ V_{(1)_q},\ V_{(2)_q},\cdots,\ V_{(q-1)_q}$ 라고 하자. 여기서 H 와 V 의 첨수들은 $\mathbf{F}_q$ 의 원소들로 생각한다. 즉

$$M_q=(V_{(0)_q},\ V_{(1)_q},\ V_{(2)_q},\ \cdots,\ V_{(q-1)_q})=(H^*,\ H_{(0)_q},\ H_{(1)_q},\ H_{(2)_q},\cdots,\ H_{(q-1)_q})^{\mathrm{T}}.$$

H^* 의 행들과 $V_{(0)_q}, V_{(1)_q}, V_{(2)_q}, \cdots, V_{(q-1)_q}$ 의 렬들을 $\mathbf{F}_q$ 의 원소들로 번호를 붙이며 $H_{(0)_q}, H_{(1)_q}, H_{(2)_q}, \cdots, H_{(q-1)_q}$ 의 행들은 $\mathbf{F}_q \setminus \{(q-1)_q\}$ 의 원소들로 번호를 붙인다.

$H_{(i)_q}$ 와 $V_{(j)_q}$ 에 의하여 결정되는 $(q-1)\times q$ 형행렬을 $(H_{(i)_q}, V_{(j)_q})$ 로 표시하자.

행렬 A 의 $(i)_q$ 행을 $(A)_{(i)_q}$, $(j)_q$ 렬을 $(A)^{(j)_q}$, $(i)_q$ 행 $(j)_q$ 렬의 원소를 $(A)_{(i)_q}^{(j)_q}$ 로, $(i)_q \in \mathbf{F}_q$ 로만 이루어진 $1\times q$ 형행렬을 $\overline{(i)_q}$ 로, $((i)_q, (i)_q+(1)_q, (i)_q+(2)_q, \cdots, (i)_q+(q-1)_q)$ 를 $\overrightarrow{(i)_q}$ 로 표시하면 행렬 M_q 를 다음과 같이 구성할수 있다.

$$(H^*)_{(i)_q} = (\overline{(i)_q}, \overline{(i)_q+(1)_q}, \overline{(i)_q+(2)_q}, \cdots, \overline{(i)_q+(q-1)_q}), \ (i)_q \in \mathbf{F}_q$$

$$(H_{(i)_q}, V_{(j)_q})_{(l)_q} = \overrightarrow{(i)_q \times ((j)_q+(1)_q)+(j)_q \times (l)_q}, \ (i)_q \in \mathbf{F}_q, \ (j)_q, (l)_q \in \mathbf{F}_q \setminus \{(q-1)_q\}$$

$$(H_{(i)_q}, V_{-(1)_q})_{(l)_q} = \begin{cases} \overrightarrow{-(l-i)_q-(i)_q}, & l \ge i \\ \overrightarrow{-(l-i+q)_q-(i-1)_q}, & l < i \end{cases}$$

보조정리 3[1, 2] 임의의 $m \in \mathbf{F}_p$ 에 대하여 갈롸체 $\mathbf{F}_p = \{0, 1, 2, \cdots, p-1\}$ 우에서의 방정식 $\begin{cases} x+y=m \\ y \ne p-1 \end{cases}$ 은 $p-1$ 개의 풀이 (x, y) 를 가지며 그중 $y \ge x$ 인 풀이는 $\frac{p-1}{2}$ 개이다. 여기서 크기관계는 대응하는 옹근수들사이의 크기관계로 생각한다.

보조정리 4 임의의 $m \in \mathbf{F}_p$ 에 대하여 갈롸체 $\mathbf{F}_p = \{0, 1, 2, \cdots, p-1\}$ 우에서의 방정식 $x+y=m$ 은 p 개의 풀이 (x, y) 를 가지며 이중에서 $x>y$ 인 풀이와 $x<y$ 인 풀이는 각각 $\frac{p-1}{2}$ 개, $x=y$ 인 풀이는 1개이다.

보조정리 5 임의의 $(a)_q, (b)_q \in \mathbf{F}_q$ 에 대하여 $\mathbf{F}_q$ 우에서의 방정식

$$(x)_q+(y)_q=(a)_q+(b)_q \times ((y-x)_q+(x)_q-(y)_q), \ y \ge x, \ y \ne q-1 \ (\text{또는 } (y)_q \ne -(1)_q) \quad (1)$$

은 $\frac{q-1}{2}$ 개의 풀이 $((x)_q, (y)_q)$ 를 가진다. 또한 방정식

$$(x)_q+(y)_q=(a)_q+(b)_q \times ((y-x+q)_q+(x-1)_q-(y)_q), \ y<x \quad (2)$$

도 $(q-1)/2$ 개의 풀이 $((x)_q, (y)_q)$ 를 가진다.

증명 첫번째 방정식에서 $((y-x)_q+(x)_q-(y)_q)$ 는 $(x)_q$ 와 $(y)_q$ 의 매 비트별크기관계에만 관계되는 상수이다.

다시말하면 $(x)_q$ 와 $(y)_q$ 의 매 비트별 크기, 작기, 같기관계만 주어지면 유일하게 결정된다. 실례로 $(y)_q$ 의 매 비트가 $(x)_q$ 의 매 비트보다 같거나 크다면

$$(y-x)_q+(x)_q-(y)_q=(0)_q.$$

만일 $(y)_q=(y_{n-1}y_{n-2}y_{n-3}\cdots y_1y_0)_p$ 와 $(x)_q=(x_{n-1}x_{n-2}x_{n-3}\cdots x_1x_0)_p$ 에 대하여

$$y_i \ge x_i \quad (i=2, \cdots, n-1), \ y_1>x_1, \ y_0<x_0$$

이면 $(y-x)_q+(x)_q-(y)_q=-(000\cdots010)_q$ 이다.

한편 식 (1)에서 마지막식을 없애여 얻어지는 방정식

$$(x)_q + (y)_q = (a)_q + (b)_q \times ((y-x)_q + (x)_q - (y)_q), \ \ y \ge x \qquad (3)$$

의 풀이

$$((x)_q,\ (y)_q) = ((x_{n-1}x_{n-2}x_{n-3}\cdots x_1x_0)_p,\ (y_{n-1}y_{n-2}y_{n-3}\cdots y_1y_0)_p)$$

들을 비트별크기관계에 따라

$$S_1 = \{((x)_q,\ (y)_q) \mid y_{n-1} > x_{n-1}\},$$
$$S_2 = \{((x)_q,\ (y)_q) \mid y_{n-1} = x_{n-1},\ y_{n-2} > x_{n-2}\},$$
$$\vdots$$
$$S_{n-1} = \{((x)_q,\ (y)_q) \mid y_{n-1} = x_{n-1},\ y_{n-2} = x_{n-2},\ y_{n-3} = x_{n-3}, \cdots,\ y_2 = x_2,\ y_1 > x_1\},$$
$$S_n = \{((x)_q,\ (y)_q) \mid y_{n-1} = x_{n-1},\ y_{n-2} = x_{n-2},\ y_{n-3} = x_{n-3}, \cdots,\ y_1 = x_1,\ y_0 \ge x_0\}$$

으로 분할할수 있다.

그리고 매 모임들은 다시 비트별 크기, 같기, 작기관계에 따라 구체적으로 분할할수 있다.

이 크기관계에 따라 식 (1)의 첫 식의 오른변은 상수로 결정된다.

보조정리 3, 4로부터 이 모임들의 크기는 다음과 같이 결정된다.

$$|S_1| = \frac{p-1}{2} \times p^{n-1},\ |S_2| = \frac{p-1}{2} \times p^{n-2}, \cdots, |S_{n-1}| = \frac{p-1}{2} \times p,\ |S_n| = \frac{p+1}{2}$$

이제 이 모임들중에서 $(y)_q = -(1)_q$ 인 풀이 하나를 제거하면 식 (1)의 풀이의 개수는

$$\frac{p-1}{2} \times (p^{n-1} + p^{n-2} + p^{n-3} + \cdots + p) + \frac{p+1}{2} - 1 =$$
$$= \frac{p-1}{2} \times (p^{n-1} + p^{n-2} + p^{n-3} + \cdots + p + 1) = \frac{p^n - 1}{2}.$$

방정식 (2)에 대하여서도 비슷한 방법으로 증명할수 있다.(증명끝)

보조정리 5와 행렬 M_q 의 구성과정으로부터 다음의 정리가 나온다.

정리 우에서 구성한 행렬 M_q 는 성질 ①, ②, ③을 만족시킨다.

다시말하면 행렬 M_q 로부터 GBTD(q, q) (GBTD(p^n, p^n)) 를 구성할수 있다.

참 고 문 헌

[1] **김일성**종합대학학보(자연과학), **58**, **12**, 7, 주체101(2012).

[2] Songchol Kim et al.; arXiv:1208.1920v1 [math.CO] 9, Aug, 2012.

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

[4] Jianxing Yin et al.; Des. Codes Cryptogr., **46**, 211, 2008.

[5] E. R. Lamken; Des. Codes Cryptogr., **11**, 37, 1997.

[6] E. R. Lamken; Trans. Am. Math. Soc., **318**, 473, 1990.

주체105(2016)년 9월 5일 원고접수

A Method to Construct Generalized Balanced Tournament Designs using Finite Fields

Kim Song Chol

We obtained a new method to construct GBTD(p^n, p^n) when p is an odd prime number and n is an integer above 2.

Key words: generalized balanced tournament design(GBTD)