김일성종합대학학보 JOURNAL OF KIM IL SUNG UNIVERSITY
(자연과학) (NATURAL SCIENCE)
주체104(2015)년 제61권 제7호 Vol. 61 No. 7 JUCHE104(2015).

일반화된 균형적시합배치의 한가지 구성법

김성철, 서진아

위대한 수령 **김일성**동지께서는 다음과 같이 교시하시였다.

《새로운 과학분야들을 개척하고 최신과학기술의 성과를 인민경제에 널리 받아들이며 중요한 기초과학부문들을 적극 발전시켜야 합니다.》(《**김일성**전집》 제27권 391페지)

우주과학기술을 발전시키는데서 통신기술 특히 통신의 보안기술을 발전시키는것이 아주 중요하다.

우주통신의 보안을 실현하는데서 주파수도약렬은 중요한 역할을 하며 일반화된 균형적시합배치(GBTD)를 리용하여 바로 이러한 주파수도약렬을 생성할수 있다.

주파수도약렬의 생성방법에 대하여서는 많은 연구가 진행되고있으며 각이한 파라메터들에 대한 GBTD의 구성방법이 해결되면 많은 문제들이 풀리게 된다.

현재까지 GBTD의 존재성 및 구성방법과 관련하여 몇가지 파라메터들에 대하여서는 여러가지 결과들이 나왔지만 아직도 많은 문제들이 미해명으로 남아있다.

모든 정수 $n \neq 2$에 대하여 GBTD(2, n)과 GBTD(3, n)이 존재하는 반면에 모든 정수 $k \geq 2$에 대하여 GBTD(k, 2)는 존재하지 않는다.[2, 3, 5] 또한 임의의 옹근수 $n \geq 5$에 대하여 GBTD(4, n)은 $n \in \{28, 32, 33, 34, 37, 38, 39, 44\}$의 경우를 제외하고 존재한다.

또한 임의의 홀씨수 p에 대하여 GBTD(p, p)가 존재한다.[1]

GBTD(2, n)과 GBTD(3, n), GBTD(4, n)의 존재성증명에서는 매 경우의 파라메터의 특성에 맞는 출발자와 첨부자를 도입하고 그것에 기초한 일반화된 균형적시합배치의 구성방법을 제기하였다.

론문에서는 일반적인 경우 즉 k와 n이 $n > k$인 임의의 옹근수인 경우 출발자와 첨부자를 도입하고 그것에 기초한 GBTD(k, n)의 구성방법에 대하여 연구하였다.

X를 υ개 원소(점)들의 모임, B를 X의 어떤 k-부분모임들의 모임이라고 하자.

만일 X의 임의의 서로 다른 두 원소쌍이 B의 λ개의 블로크에 속하면 순서쌍 (X, B)를 균형적불완전블로크배치라고 부르고 (υ, k, λ)-BIBD로 표시한다.

(υ, k, λ)-BIBD의 블로크수는 $\lambda\binom{\upsilon}{2}\Big/\binom{k}{2} = \dfrac{\lambda\upsilon(\upsilon-1)}{k(k-1)}$이며[2] $(kn, k, k-1)$-BIBD의 블로크수는 $n(kn-1)$이다.

만일 어떤 $(kn, k, k-1)$-BIBD (X, B)에 대하여 B의 블로크들을 다음의 두가지 조건이 만족되도록 $n \times (kn-1)$배렬로 배치할수 있다면 (X, B)를 일반화된 균형적시합배치라고 부르고 GBTD(k, n)으로 표시한다.

i) X의 모든 점은 매 렬의 꼭 1개 블로크에 포함된다.

ii) X의 모든 원소들은 매 행의 기껏 k개 블로크에 포함된다.

정의로부터 일반화된 균형적시합배치를 대응하는 블로크배렬로 생각할수 있다.

보조정리 1 [4] GBTD(k, n)의 모든 점은 $(n-1)$개 행에는 k번 포함되며 나머지 한행에는 $(k-1)$번 포함된다.

G를 X 우에서의 GBTD(k, n)이라고 하자.

G의 i번째 행에 $(k-1)$번만 포함되는 원소를 i번째 행의 부족점이라고 부른다.

G의 매 행은 꼭 k개의 부족점을 가진다는것을 쉽게 알수 있다.

이 k개의 부족점들을 i번째 행의 부족$k-$원소조라고 부른다.

보조정리 2 GBTD(k, n)의 부족$k-$원소조들은 점모임들로 분할된다.

$n > k$일 때 출발자와 첨부자에 의한 GBTD(k, n)의 구성방법에 대하여 론의하자.

이제부터 모임들은 다중모임들로 생각한다.

일반화된 균형적시합배치를 위한 출발자, 첨부자를 아래와 같이 정의한다.

편리상 GBTD(k, $n+1$)을 위한 출발자, 첨부자를 정의하자.

$n+1 > k$라고 하고 다음의 기호들을 약속한다.

$$m := n - k + 1$$

$$B_i := \{\infty_i,\ y_{i1},\ \cdots,\ y_{ik-1}\},\ \ y_{il} \in Z_{nk},\ l = 1,\ 2, \cdots,\ k-1,\quad i = 1,\ 2, \cdots,\ k$$

$$B_{i+k} := \{x_{i1},\ x_{i2}, \cdots,\ x_{ik}\},\ \ x_{il} \in Z_{nk},\ \ l = 1,\ 2, \cdots,\ k,\quad i = 1,\ 2, \cdots,\ m$$

모임 B_i들이 조건 $\bigcup_{i=1}^{n+1} B_i = Z_{nk} \cup \{\infty_1,\ \infty_2, \cdots,\ \infty_k\}$를 만족시킨다고 하자.

이제 매 블로크 B_i에 대해서 Δ_i를 다음과 같이 정의하자.

$$\Delta_i := \{y_{il} - y_{ij} \mid 1 \le l,\ \ j \le k-1,\quad l \ne j\},\ \ i = 1,\ 2, \cdots,\ k$$

$$\Delta_{i+k} := \{x_{il} - x_{ij} \mid 1 \le l,\ \ j \le k,\ \ l \ne j\},\ \ i = 1,\ 2, \cdots,\ m$$

모임 D_i들을 다음과 같이 정의하자.

$$D_0 := \{0,\ n,\ 2n, \cdots,\ (k-1)n\}$$

$$D_i := D_0 + i\ ,\ \ i = 0,\ 1, \cdots,\ n-1$$

여기서 $D_0 + i$는 D_0의 매 원소와 i의 합으로 이루어진 모임을 의미한다.

이때 $\bigcup_{i=1}^{n+1} \Delta_i = (k-1)(Z_{nk} - D_0)$이면(오른변은 Z_{nk}에서 D_0을 던 차모임의 원소들로 이루어지고 매 원소들의 중복도가 $k-1$인 다중모임을 의미한다.) $S = (B_1,\ B_2, \cdots,\ B_{n+1})$을 $Z_{nk} \cup \{\infty_1, \infty_2, \cdots,\ \infty_k\}$우에서 정의된 GBTD($k$, $n+1$)을 위한 출발자라고 부른다.

더우기 $A = (a_1,\ a_2, \cdots, a_n)$이 Z_n의 서로 다른 원소들로 이루어져있고 $\bigcup_{i=1}^{n} (B_i + a_i)$가 D_j ($j = 0,\ 1, \cdots, n-1$)의 최대로 k개의 원소(반드시 다르지는 않은)를 포함하면 A를 출발자 S에 대한 첨부자라고 부른다.

출발자, 첨부자에 의한 GBTD(k, $n+1$)의 구성과정을 다음의 정리로 보여준다.

정리 $Z_{nk} \cup \{\infty_1, \infty_2, \cdots,\ \infty_k\}$우에서 정의된 GBTD($k$, $n+1$)을 위한 출발자 S와 그에 대한 첨부자 A가 존재하면 GBTD(k, $n+1$)이 존재한다.

증명 $Z_{nk}\bigcup\{\infty_1, \infty_2, \cdots, \infty_k\}$ 우에서의 $(n+1)\times(nk+k-1)$ 배렬 G 를 다음과 같이 구성하자.

G 의 행번호를 $0, 1, \cdots, n$ 으로, 렬번호를 $0, 1, \cdots, nk+k-2$ 로 붙이자.

이제 $i=1,\cdots, n,\ j=0, \cdots, n-1,\ l=0, \cdots, k-1$ 에 대하여 G 의 $(j,\ (a_i+ln+j) \bmod nk)$ 원소를 B_i+a_i+ln+j 로 놓는다.

$j=0, 1, \cdots, nk-1$ 에 대하여 G 의 $(n,\ j)$ 원소를 $B_{n+1}+j$ 로 놓는다.

$l=1, 2, \cdots, k-1$ 에 대하여 G 의 $(n,\ nk-1+l)$ 원소를 $\{\infty_1, \infty_2, \cdots, \infty_k\}$ 로 놓는다.

첨부자 A 의 정의에 의하여 모임

$$kZ_{nk}-\{B_i+a_i+ln \mid i=1, 2, \cdots, n,\ \ l=0, 1, \cdots, k-1\}$$

은(반드시 다르지는 않은) k 개의 모임 $D_{i_1}, D_{i_2}, \cdots, D_{i_k}$ 로 분할할수 있다.

$l=1, 2, \cdots, k-1$ 에 대하여 G 의 $(j,\ nk-1+l)$ 원소를 $D_{i_l}+j$ 로 놓는다.

이렇게 정의된 배렬 G 는 $Z_{nk}\bigcup\{\infty_1, \infty_2, \cdots, \infty_k\}$ 우에서 정의된 GBTD$(k,\ n+1)$ 이다.

G 의 첫 렬의 블로크모임은 $[S]$ 이다.(여기서 $[S]$ 는 S 에 속하는 블로크들의 모임을 의미한다.)

$j=0, 1, \cdots, nk-1$ 에 대하여 G 의 j 렬의 블로크모임은 $[S]+j$ 이다.

$j=nk,\ nk+1,\ \cdots,\ nk+k-2$ 에 대하여 G 의 j 렬의 블로크모임들의 합은

$$\bigcup_{i=0}^{n-1} D_i \bigcup\{\infty_1,\ \infty_2, \cdots,\ \infty_k\}.$$

따라서 $Z_{nk}\bigcup\{\infty_1, \infty_2, \cdots, \infty_k\}$ 의 모든 원소는 G 의 매 렬에서 꼭 한번씩 나타난다.

첨부자 A 의 정의로부터 $Z_{nk}\bigcup\{\infty_1, \infty_2, \cdots, \infty_k\}$ 의 모든 원소들은 G 의 매 행에서 최대로 k 번 나타난다.

부족원소조들은 $\{D_{i_k}+j \mid j=0, 1, \cdots,\ n-1\}\bigcup\{\infty_1,\ \infty_2, \cdots,\ \infty_k\}$ 이다.

마지막으로 우와 같이 정의한 G 가 $((n+1)k,\ k,\ k-1)-$BIBD 라는것을 증명하기 위하여 $\{x,\ y\}$ $(x,\ y\in Z_{nk}\bigcup\{\infty_1,\ \infty_2, \cdots,\ \infty_k\},\ x\neq y)$ 가 G 의 꼭 $(k-1)$ 개 블로크에 포함되여있음을 증명하자.

$x,\ y\in Z_{nk}$ 인 경우 $x\not\equiv y(\bmod n)$ 이면 S 의 정의로부터 렬번호가 0인 블로크들(즉 $[S]$)에는 $x'-y'=x-y$ 인 $\{x',\ y'\}$ 가 $(k-1)$ 번 포함된다.

따라서 번호가 0인 렬부터 번호가 $(nk-1)$ 인 렬까지의 블로크들 즉

$$[S]\bigcup([S]+1)\bigcup([S]+2)\bigcup\cdots\bigcup([S]+nk-1)$$

에는 $\{x,\ y\}$ 가 $(k-1)$ 번 포함된다.

또한 $x\equiv y(\bmod n)$ 이면 $\{x,\ y\}$ 는 $j=nk,\ nk+1, \cdots,\ nk+k-2$ 에 대하여 매 렬 j 의 꼭 1개 블로크 즉 총 $(k-1)$ 개 블로크에 포함된다.

다음으로 $x,\ y$ 들중 하나가 ∞_i 인 경우에 대하여 보자.

일반성을 잃지 않고 $x=\infty_i,\ y\in Z_{nk}$ 라고 하자.

렬 0에는 x 즉 ∞_i 를 포함하는 블로크가 꼭 하나 있다.

그 블로크를 $\{\infty_i,\ a_1,\ a_2,\ a_3, \cdots,\ a_{k-1}\}$ 이라고 하자. 여기서 $a_i\in Z_{nk},\ i=1, \cdots, k-1$.

G 의 구성으로부터 렬 $j\ (0\le j\le nk-1)$ 에서 ∞_i 가 포함되여있는 블로크는

$$\{\infty_i,\ a_1+j,\ a_2+j,\ a_3+j, \cdots,\ a_{k-1}+j\}.$$

이 블로크들중 y가 포함되여있는 블로크는 분명히 $(k-1)$개이다.

$x,\ y \in \{\infty_1,\ \infty_2,\ \cdots,\ \infty_k\}$인 경우 G의 구성으로부터 모든 $l=1,\ 2,\ \cdots,\ k-1$에 대하여 $(n,\ nk-1+l)$위치의 블로크들은 $\{\infty_1,\ \infty_2,\ \cdots,\ \infty_k\}$이다.

이로부터 G는 $((n+1)k,\ k,\ k-1)-\mathrm{BIBD}$이다.(증명끝)

정리로부터 일반화된 균형적시합배치를 위한 출발자와 첨부자가 존재하면 그로부터 일반화된 균형적시합배치를 구성할수 있다는것을 알수 있다.

참고문헌

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

[2] C. J. Colbourn et al.; The CRC Handbook of Combinatorial Designs, CRC Press, 22～45, 2007.

[3] E. R. Lamken; Des. Codes Cryptogr., 3, 33, 1992.

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

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

주체104(2015)년 3월 5일 원고접수

A Construction Method of Generalized Balanced Tournament Designs

Kim Song Chol, So Jin A

A generalized balanced tournament design, or a $\mathrm{GBTD}(k,\ n)$ in short, is a $(kn,\ k,\ k-1)$ −BIBD defined on a kn-set X.

Its blocks can be arranged into an $n\times(kn-1)$ array in such a way that (1) every element of X is contained in exactly one cell of each column, and (2) every element of X is contained in at most k cells of each row.

We present a new construction for $\mathrm{GBTD}(k,\ n)$s by starter-adder method.

Key word: generalized balanced tournament design