김일성종합대학학보 (자연과학) 주체104(2015)년 제61권 제3호
JOURNAL OF **KIM IL SUNG** UNIVERSITY (NATURAL SCIENCE) Vol. 61 No. 3 JUCHE104(2015).

GBTD(4, 2)의 비존재성

김 성 철

위대한 령도자 **김정일**동지께서는 다음과 같이 교시하시였다.

《과학기술을 발전시켜야 나라의 경제를 빨리 추켜세울수 있으며 뒤떨어진 기술을 앞선 기술로 갱신하여 생산을 끊임없이 높여나갈수 있습니다.》(《**김정일**선집》 증보판 제20권 62페지)

$\text{GBTD}(k,\ m)$은 블로크들을 다음의 두가지 조건이 만족되도록 $m\times(km-1)$배렬로 배치가능한 $km-$모임 V우에서의 $(km,\ k,\ k-1)-\text{BIBD}$이다.

i) V의 모든 원소는 매 렬의 꼭 1개 세포에 포함된다.

ii) V의 모든 원소는 매 행의 기껏 k개 세포에 포함된다.

조건 (1)은 $\text{GBTD}(k,\ m)$이 RBIBD라는것을 말해준다.

선행연구[2]에서는 $k=2,\ 3$인 경우의 $\text{GBTD}(k,\ m)$의 존재성을 밝혔으며 선행연구[1]에서는 $k=4$, $m\notin\{2,\ 3,\ 4,\ 28,\ 32,\ 33,\ 34,\ 37,\ 38,\ 39,\ 44\}$인 경우의 존재성을 밝혔다.

론문에서는 $k=4$, $m=2$인 경우 즉 $\text{GBTD}(4,\ 2)$의 존재성문제를 론의하였다.

$\text{GBTD}(4,\ 2)$는 우의 두가지 조건을 만족시키는 $(8,\ 4,\ 3)-\text{RBIBD}$이다.

여기서는 $(8,\ 4,\ 3)-\text{RBIBD}$가 동형성의 견지에서 유일하다는것을 밝히고 이에 기초하여 $\text{GBTD}(4,\ 2)$가 존재하지 않는다는것을 밝혔다.

1. 기초개념

V를 원소가 v개인 모임, B를 V의 어떤 $k-$부분모임(블로크)들의 모임이라고 하자.

만일 V의 임의의 서로 다른 두 원소쌍이 B의 꼭 λ개의 블로크들에 속하면 순서붙은 쌍 $(V,\ B)$를 $(v,\ k,\ \lambda)$ ─균형적불완전블로크배치(balanced incomplete block design), 또는 $(v,\ k,\ \lambda)-\text{BIBD}$라고 부른다.

$(V_1,\ B_1)$, $(V_2,\ B_2)$에 대하여 만일 어떤 우로의 1∶1넘기기 $\alpha: V_1\to V_2$가 존재하여 $\alpha(B_1)=B_2$이면 두 BIBD는 동형이라고 말한다. 여기서 α는 B_1의 블로크들의 개별적인 점들에 각각 작용한다.

배치 $(V,\ B)$에서 B의 어떤 부분모임 C에 대하여 C가 점모임 V의 분할로 되면 C를 병렬클라스(parallel class) 혹은 분해클라스(resolution class)라고 부른다.

또한 블로크들의 모임을 병렬클라스들로 분할할수 있는 $(v,\ k,\ \lambda)-\text{BIBD}$를 분해가능한 균형적불완전블로크배치(resolvable balanced incomplete block design)라고 부르고 $(v,\ k,\ \lambda)-\text{RBIBD}$로 표시한다.

정의로부터 $(v,\ k,\ \lambda)-\text{BIBD}$는 블로크를 $\dfrac{\lambda v(v-1)}{k(k-1)}$개 포함한다.

$(km,\ k,\ k-1)-\text{BIBD}$는 블로크를 $m(km-1)$개 포함한다.

만일 어떤 $(km,\ k,\ k-1)-\text{BIBD}$ $(X,\ \boldsymbol{A})$에 대하여 $\boldsymbol{A}$의 블로크들을 다음의 두가지 조건이 만족되도록 $m\times(km-1)$ 배렬로 배치할수 있다면 $(X,\ \boldsymbol{A})$를 일반화된 균형적경기배치(generalized balanced tournament design)라고 부르고 간단히 $\text{GBTD}(k,\ m)$으로 표시한다.

(1) X의 모든 점은 매 렬에서 꼭 한번 나타난다.

(2) X의 모든 점은 매 행의 기껏 k개 세포에 포함된다.

조건 (1)은 $\text{GBTD}(k,\ m)$이 추가적인 제한조건을 가진 $(km,\ k,\ k-1)-\text{RBIBD}$라는것을 말해준다.

정의로부터 GBTD를 대응하는 블로크들의 배렬로 생각할수 있다.

보조정리 1 [3] $\text{GBTD}(k,\ m)$의 모든 점은 $(m-1)$개 행들에는 k번 포함되며 나머지 한 행에는 $(k-1)$번 포함된다.

$n\times n$ (± 1) −행렬 H에 대하여 $HH^T=nI$ (모든 행들이 둘씩 직교)이면 H를 차수가 n인 아다마르행렬이라고 부른다.

두 아다마르행렬에 대하여 한 행렬을 다른 행렬에 행 또는 렬들의 치환, 행 또는 렬의 부호바꾸기를 유한번 실시하여 얻을수 있다면 두 아다마르행렬은 동등하다고 말한다.

만일 어떤 아다마르행렬의 첫 행과 첫 렬의 원소들이 모두 1이면 그 아다마르행렬은 정규화된 아다마르행렬이라고 부른다.

분명히 모든 아다마르행렬은 우에서 서술한 변환들을 리용하여 정규화할수 있다.

RBIBD와 아다마르행렬사이에 다음의 관계가 성립된다.

보조정리 2 $(4n,\ 2n,\ 2n-1)-\text{RBIBD}$는 $4n$차아다마르행렬과 동등하다.

$\{1,\ 2,\ \cdots,\ 4n\}$을 정점모임, $4n$차정규아다마르행렬의 첫 행을 제외한 매 나머지 행들에서 +1이 들어있는 렬번호들의 모임, −1이 들어있는 렬번호들의 모임들을 블로크들로 하면 $(4n,\ 2n,\ 2n-1)-\text{RBIBD}$가 얻어진다.

거꾸로 $(4n,\ 2n,\ 2n-1)-\text{RBIBD}$로부터 아다마르행렬을 구축할수 있다.

실례 4차정규아다마르행렬

$$\begin{pmatrix} + & + & + & + \\ + & - & + & - \\ + & + & - & - \\ + & - & - & + \end{pmatrix}$$

에 대응하는 $(4,\ 2,\ 1)-\text{RBIBD}$ $(V,\ B)$는

$$V=\{1,\ 2,\ 3,\ 4\},$$
$$B=\{\{1,\ 3\},\ \{2,\ 4\},\ \{1,\ 2\},\ \{3,\ 4\},\ \{1,\ 4\},\ \{2,\ 3\}\}.$$

2. $\text{GBTD}(k,\ m)$의 존재성결과들

$\text{GBTD}(k,\ m)$은 부호리론과 밀접히 련관되여있으며 특히 $\text{GBTD}(k,\ m)$으로부터 쁠로뜨낀경계에 도달하는 최량 NCCC부호를 구축할수 있다.[1]

이로부터 $\text{GBTD}(k,\ m)$의 존재성에 대하여 많은 연구가 진행되였다.

$m>2$일 때 $\text{GBTD}(2,\ m)$, $\text{GBTD}(3,\ m)$이 존재하며 $\text{GBTD}(2,\ 2)$, $\text{GBTD}(3,\ 2)$는 존재하지 않는다.[2]

또한 $m\geq 5$, $m\notin\{28,\ 32,\ 33,\ 34,\ 37,\ 38,\ 39,\ 44\}$일 때 $\text{GBTD}(4,\ m)$이 존재한다는것이 밝

혀졌다.[1]

한편 모든 k에 대하여 GBTD$(k, 1)$은 분명히 존재한다.

그러나 $k=4$, $m \in \{2, 3, 4, 28, 32, 33, 34, 37, 38, 39, 44\}$인 경우의 존재성에 대하여서는 아직 밝혀진것이 없다.

$k=4$, $m=\{2, 3, 4\}$인 경우의 존재성문제를 해결하면 $m=37$인 경우를 제외한 나머지 7가지 경우의 존재성문제를 쉽게 해결할수 있다.[2]

이로부터 론문에서는 $k=4$, $m=2$인 경우 즉 GBTD(4, 2)의 비존재성을 밝혔다.

3. GBTD(4, 2)의 비존재성

GBTD(4, 2)는 조건 i), ii)를 만족시키는 (8, 4, 3)−RBIBD이다.

한편 보조정리 2로부터 (8, 4, 3)−RBIBD는 8차아다마르행렬과 동등하다.

보조정리 3 8차아다마르행렬은 동등성의 견지에서 유일하게 존재한다. 즉 모든 8차아다마르행렬들은 아다마르행렬

$$\begin{pmatrix} + & + & + & + & + & + & + & + \\ + & + & - & - & + & + & - & - \\ + & - & + & - & + & - & + & - \\ + & - & - & + & + & - & - & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & - & - & + & + \\ + & - & + & - & - & + & - & + \\ + & - & - & + & - & + & + & - \end{pmatrix}$$

와 동등하다.

증명 모든 아다마르행렬들은 아다마르행렬의 정의로부터 분명히 우에서 서술한 변환들, 즉 행 또는 렬의 치환, 행 또는 렬의 부호바꾸기에 의해 첫 3개 행이 다음과 같은 정규화된 아다마르행렬로 만들수 있다.

$$\begin{pmatrix} + & + & + & + & + & + & + & + \\ + & + & + & + & - & - & - & - \\ + & + & - & - & + & + & - & - \end{pmatrix}$$

이 3개의 행들과 동시에 직교하면서 첫 원소가 +인 가능한 행들은 다음과 같다.

$$\begin{array}{llllllll l} 1 & + & + & - & - & - & - & + & + \\ 2 & + & - & + & - & + & - & + & - \\ 3 & + & - & + & - & + & - & - & + \\ 4 & + & - & + & - & - & + & + & - \\ 5 & + & - & + & - & - & + & - & + \\ 6 & + & - & - & + & + & - & + & - \\ 7 & + & - & - & + & + & - & - & + \\ 8 & + & - & - & + & - & + & + & - \\ 9 & + & - & - & + & - & + & - & + \end{array}$$

이 9개의 행들중에서 서로 직교하는 행들은 기껏 5개 선택할수 있다.

행 1은 나머지 8개의 행들과 직교한다.

행 2－9들은 각각 행 2－9들중 4개의 행들과 직교하지 않는다.

이로부터 행 2－9중에서 기껏 4개의 행들이 선택가능하다.

9개 행들중에서 가능한 5개의 서로 직교하는 행들의 가능한 조는

$$\{1,\ 2,\ 5,\ 7,\ 8\},\ \{1,\ 3,\ 4,\ 6,\ 9\}.$$

한편 행 2, 5, 7, 8의 렬 3과 4를 바꾸면 각각 행 6, 9, 3, 4로 된다.

이로부터 나머지 5개의 행들이 우의 두가지 경우로 되는 모든 정규아다마르행렬들, 다시말하면 모든 아다마르행렬들은 동등하다는것이 나온다.(증명끝)

정리 GBTD(4, 2) 는 존재하지 않는다.

증명 정규아다마르행렬에서 두 렬 i , j 의 자리바꾸기는 대응되는 RBIBD 들사이의 $\alpha(i)=j,\ \alpha(j)=i,\ \alpha(k)=k,\ k\neq i,\ j$ 와 같은 동형넘기기에 대응된다. 그리고 두 렬의 자리바꾸기, 행의 부호바꾸기는 얻어지는 대응되는 RBIBD 에 영향을 주지 않는다. 따라서 동등한 8차정규아다마르행렬들로부터 얻어지는 (8, 4, 3)－RBIBD 들은 동형이다.

이 사실과 보조정리 3으로부터 모든 (8, 4, 3)－RBIBD 들은 다음의 (8, 4, 3)－RBIBD $(V,\ B)$ 와 동형이다.

$$V=\{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8\}$$

$$B=\{\{1,\ 2,\ 4,\ 5\},\ \{3,\ 4,\ 7,\ 8\},\ \{1,\ 3,\ 5,\ 7\},\ \{2,\ 4,\ 6,\ 8\},\ \{1,\ 4,\ 5,\ 8\},\ \{2,\ 3,\ 6,\ 7\},$$
$$\{1,\ 2,\ 3,\ 4\},\ \{5,\ 6,\ 7,\ 8\},\ \{1,\ 2,\ 7,\ 8\},\ \{3,\ 4,\ 5,\ 6\},\ \{1,\ 3,\ 6,\ 8\},$$
$$\{2,\ 4,\ 5,\ 7\},\ \{1,\ 4,\ 6,\ 7\},\ \{2,\ 3,\ 5,\ 8\}\}$$

간단한 검토를 통하여 동형의 견지에서 유일한 우의 (8, 4, 3)－RBIBD $(V,\ B)$ 가 GBTD(4, 2) 가 아니라는것을 알수 있다.(증명끝)

참 고 문 헌

[1] Yin Jian Xing et al.; Des. Codes Cryptogr., 46, 211, 2008.

[2] E. R. Lamken; Des. Codes Cryptgr., 11, 37, 1997.

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

주체103(2014)년 11월 5일 원고접수

The Nonexistence of GBTD(4, 2)

Kim Song Chol

We show that there is exactly one RBIBD(8, 4, 3) up to isomorphism, and from this result there is no GBTD(4, 2).

Key words: design, GBTD, RBIBD