김일성종합대학학보
수 학

주체109(2020)년
제66권 제2호

n이 씨수제곱일 때 일반화된 균형적시합배치 GBTD(n, n)의 구성알고리듬

김 성 철

론문에서는 차분행렬을 리용하여 n이 씨수의 제곱일 때 일반화된 균형적시합배치 GBTD(n, n)을 구성하는 알고리듬을 연구하였다.

일반화된 균형적시합배치는 전력선통신을 비롯하여 최근의 통신에서 많이 리용되는 동등기호무게부호의 구성에 중요하게 리용되는것으로 하여 그것의 존재성과 구성법을 밝히는것이 중요한 문제로 되고있다.[2, 3]

선행연구[3]에서는 n이 홀씨수의 제곱일 때 차분행렬을 리용하여 GBTD(n, n)을 구성하는 방법을 제기하였다. 선행연구[1]에서는 선행연구[3]에서 해결하지 못한 문제로서 n이 2의 제곱인 경우의 구성법을 제기하였다.

론문에서는 n이 씨수의 제곱인 경우 선행연구에서 해결한 두가지 방법들을 연구하고 하나의 알고리듬으로 구성할수 있는 방법론을 제기하였다.

아래의 서술에서 다음의 표기들을 리용한다.

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

$\mathbf{F}_n$은 위수가 n인 유한체이다.

보조정리 1[3] 만일 위수가 n인 가법군우에서의 균일한 $(n, n, n-1)-DM$이 존재하면 $G\times\mathbf{Z}_n$우에서의 GBTD(n, n)이 존재한다.

보조정리 2[3] $n=p^q$(여기서 p는 홀씨수)일 때 균일한 $(n, n, n-1)-DM$이 존재한다.

증명 주어진 홀씨수제곱 n에 대하여 G를 원시원소가 w인 유한체 $\mathbf{F}_n$의 더하기군으로 취한다. $\mathbf{F}_n$우에서 $n\times n$형배렬을 구성한다.

$$D=\begin{pmatrix} d_{xy} \\ -y^2 \end{pmatrix}$$

여기서 $d_{xy}=2xy+x^2$, $x\in\mathbf{F}_n\setminus\{0\}$, $y\in\mathbf{F}_n$이다. D의 매 행이 령을 꼭 한번 포함한다는것은 쉽게 검사할수 있다. D의 임의의 서로 다른 두 행의 벡토르차도 령을 꼭 한번 포함한다. 따라서 $\mathbf{F}_n$우에서의 균일한 $(k, k, k-1)-DM$은 다음의 배렬을 취하여 구성할수 있다.

$$D^*=(1\cdot D\,|\,w\cdot D\,|\,w^2\cdot D\,|\cdots|\,w^{k-2}\cdot D)$$

(증명끝)

보조정리 3[1] $n=2^k$, $k\geq 2$일 때 균일한 $(n, n, n-1)-DM$이 존재한다.

우의 보조정리들로부터 다음의 정리가 곧 나온다.

정리 $n=2^k$, $k\geq 2$일 때 GBTD(n, n)이 존재한다.

선행연구결과들을 보면 n이 씨수제곱일 때 GBTD(n, n)의 구성은 보조정리 1, 2에서의 균일한 $(n, n, n-1)-DM$의 구성에 기초하여 진행된다. 그러나 보조정리 1, 2의 증명

에서 구성과정들을 보면 n이 홀씨수의 제곱인가 2의 제곱인가에 따라 큰 차이가 있으며 따라서 경우에 따라 전혀 다른 알고리듬으로 균일한 차분행렬을 구성해야 하는 결함을 가진다.

론문에서는 우의 두가지 경우에 한가지 알고리듬을 리용하여 균일한 차분행렬을 구성하며 본래의 방법에 비하여 계산량적으로 우월한 방법을 연구하였다. 그 방법은 보조정리 3의 구성적증명과정에 기초하고있다.

보조정리 4 $n>2$가 씨수제곱일 때 균일한 $(n,\ n,\ n-1)-DM$이 존재한다.

증명 G를 유한체 $\mathbf{F}_n=\mathbf{Z}_p[x]/(g(x))$의 가법군으로 취한다. 여기서 $g(x)\in\mathbf{Z}_p[x]$는 q차기약다항식이다. $\mathbf{F}_n$의 원소들은 $\mathbf{Z}_p[x]$의 차수가 기껏 $k-1$인 다항식으로 표현된다.

편리상 $\mathbf{F}_n$의 원소

$$0,\ 1,\ \cdots,\ p-1,\ x,\ x+1,\ \cdots,\ (p-1)x^{q-1}+(p-1)x^{q-2}+\cdots+(p-1)$$

들을 각각 $a_0,\ a_1,\ a_2,\ a_3,\ \cdots,\ a_{n-1}$로 표시하겠다.

$\mathbf{F}_n$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 다음의 행렬 역시 차분행렬이다.

$$D^{*1}=(D_1\,|\,D_2\,|\,D_3\,|\cdots|\,D_{n-1})$$

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}이라고 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. 그리고 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.

$\{j_1-a_1,\ j_2-a_2,\ \cdots,\ j_{n-1}-a_{n-1}\}=\{j_1,\ j_2,\ \cdots,\ j_{n-1}\}$이도록 하기 위하여 $j_i,\ i=\overline{1,\ n-1}$들을 다음과 같은 $\mathbf{F}_n$우의 련립1차방정식의 풀이로 놓는다.

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

이 련립1차방정식은 다음과 같은 풀이를 가진다.

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

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 다음과 같다고 하자.

$$D^{*2}=(D_1'\,|\,D_2'\,|\,D_3'\,|\cdots|\,D_{n-1}')$$

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_i렬의 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 $(8,\ 8,\ 7)-DM$이다.(증명끝)

보조정리 4의 증명과정에서의 구성방법에 따라 균일한 차분행렬을 구성한다고 하면 보조정리 2, 3의 구성방법에 따라 두가지 경우에 서로 다른 방법으로 구성하는것에 비하여 통일적인 방법으로 구성할수 있다는 우점을 가진다.

그리고 보조정리 4의 구성방법은 보조정리 3의 구성방법의 일반화로서 n이 2의 제곱인 경우에는 이 방법들은 같게 된다. 한편 보조정리 2의 구성방법으로 균일한 차분행렬을 구성하려면 D를 구성하려고 해도 곱하기를 대략 $2n^2$정도의 곱하기와 n^2정도의 곱하기를 필요로 하며 D로부터 균일한 차분행렬 D^*을 얻으려면 대략 n^3정도의 곱하기를 필요로 한다.

이에 비하여 보조정리 4의 구성방법으로 균일한 차분행렬을 구성하려면 n^2정도의 곱하기와 $2n^2$정도의 더하기면 충분하다.

이상과 같이 보조정리 4를 리용하면 n이 씨수의 제곱인 경우 n이 짝수인 경우와 홀수인 경우 두가지 경우로 갈라서 하던 선행방법에 비하여 한가지 방법으로 GBTD(n, n)의 구성에 필요한 균일한 차분행렬을 쉽게 얻을수 있다.

참 고 문 헌

[1] **김일성**종합대학학보 수학, 65, 4, 24, 주체108(2019).

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

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

주체108(2019)년 12월 15일 원고접수

An Algorithm to Construct Generalized Balanced Tournament Designs GBTD(n, n) when n be a Prime Power

Kim Song Chol

In this paper, we present an algorithm to construct generalized balanced tournament designs GBTD(n, n) when $n > 2$ is a prime power, using difference matrices.

Keywords: generalized balanced tournament design(GBTD), difference matrix