그런데 명제 3에 의하여 F_q의 임의의 비자명한 더하기지표 ψ에 대하여

$$\left|\sum_{x\in D}\psi(x)\right| = \left|\frac{\sum_{x\in F_q}\psi(x)-1}{m}\right| \le \frac{(m-1)\sqrt{q}+1}{m} < \sqrt{q}$$

이다. 따라서 $|D| > 6s\sqrt{q}$ 즉 $m < (q-1)/(6s\sqrt{q})$ 이면 정리 1을 적용하여 다음의 결과를 얻을수 있다.

정리 2 m을 $m < (q-1)/(6s\sqrt{q})$인 정의 옹근수, D를 F_q^*의 지표 m인 부분군(여기서 $q=2^s$, $s \ge 1$이다.), k는 $\frac{|D|}{3} < k \le \frac{|D|}{2} - \sqrt{q}$인 정의 옹근수라고 하자.

이때 임의의 $b \in F_q$에 대하여 $N_D(k,\ b) > 0$이다.

참 고 문 헌

[1] 김률; 유한체, **김일성**종합대학출판사, 250～300, 주체100(2011).

[2] G. Zhu et al.; Finite Fields Appl., 18, 192, 2012.

[3] J. Li et al.; Sci. China Math., 53, 9, 2351, 2010.

[4] J. Li et al.; Finite Fields Appl., 14, 911, 2008.

[5] W. Wang; J. Nguyen Finite Fields Appl., 51, 204, 2018.

[6] W. Wang et al.; Finite Fields Appl., 43, 106, 2017.

주체108(2019)년 3월 15일 원고접수

The $k-$Subset Sum Problem over Finite Fields of Characteristic 2

Choe Hyok, Choe Chung Hyok

We study the $k-$subset sum problem over finite fields and improve the previous results for this problem in the case of characteristic 2.

Key words: subset sum, additive character

김일성종합대학학보 주체108(2019)년
수 학 제65권 제3호

차분행렬을 리용한 일반화된 균형적시합배치의 구성

김 성 철

론문에서는 아직까지 미해결로 남아있는 경우인 n이 2의 제곱인 경우 GBTD$(n,\ n)$의 존재성문제를 해결하기 위하여 차분행렬을 리용하여 n이 4인 경우와 8인 경우 즉 GBTD(4, 4)와 GBTD(8, 8)을 구성하였다.

선행연구[1]에서는 $k=2,\ 3$인 경우, 선행연구[3, 6]에서는 $k=4$인 경우, 선행연구[4]에서는 $k=5$인 경우 GBTD$(k,\ m)$의 존재성을 연구하였으며 차분행렬을 리용하여 n이 홀씨수의 제곱일 때 GBTD$(n,\ n)$의 구성법을 제안하였다.

선행연구[5]에서는 GBTD$(k,\ k)$와 동등한 k^2차행렬을 도입하여 p가 홀씨수이고 n이 2이상의 옹근수일 때 GBTD$(p^n,\ p^n)$을 구성하였다.

정의 1[1] V를 원소(점이라고 부른다.)가 v개인 모임, B를 V의 어떤 k－부분모임(블로크라고 부른다.)들의 모임이라고 하자.

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

보조정리 1[2] $(v,\ k,\ \lambda)-$BIBD는 블로크를 $\lambda v(v-1)/[k(k-1)]$개 가진다. 즉 $(km,\ k,\ k-1)-$BIBD는 블로크를 $m(km-1)$개 가진다.

정의 2[1] 어떤 $(km,\ k,\ k-1)-$BIBD $(V,\ B)$에 대하여 B의 블로크들을 다음의 두가지 조건을 만족시키는 $(m\times(km-1))$형행렬로 배렬할수 있다면 $(V,\ B)$를 일반화된 균형적시합배치(Generalized Balanced Tournament Design)라고 부르고 GBTD$(k,\ m)$으로 표시한다.

① V의 모든 점은 매 렬의 꼭 1개 블로크에 포함된다.

② V의 모든 점은 매 행의 기껏 k개 블로크에 포함된다.

GBTD$(k,\ m)$은 블로크들을 점모임의 모든 원소는 조건 ①, ②를 만족시키도록 $(m\times(km-1))$형행렬로 배렬할수 있는 균형적불완전블로크배치 $(km,\ k,\ k-1)-$BIBD이다.

정의 2에 의하여 GBTD는 그것에 대응되는 블로크들의 배렬로 생각할수 있다.

정의 3[4] G를 위수가 v인 가법군이라고 하자.

G우에서의 $(k\times\lambda v)$형행렬 D에 대하여 만일 D의 임의의 서로 다른 두 행 $R_i,\ R_j$에 대하여 차벡토르 R_j-R_i가 G의 모든 원소들을 꼭 λ번씩 포함하면 차분행렬이라고 부르고 $(v,\ k,\ \lambda)-$DM으로 표시한다.

어떤 차분행렬에 대하여 그 행렬의 매 행들이 G의 모든 원소들을 꼭 λ번씩 포함하면 균일한 차분행렬이라고 부른다.

정의옹근수 $m\neq 2$에 대하여 GBTD$(2,\ m)$, GBTD$(3,\ m)$이 존재하며[1] 옹근수 $k\geq 2$에 대하여 GBTD$(k,\ 2)$는 존재하지 않는다.[6] $m\neq 2,\ 3$인 정의 옹근수 m에 대하여 GBTD$(4,\ m)$은 존재하며 GBTD(4, 2)와 GBTD(4, 3)은 존재하지 않는다.[3, 11]

$m \ge 62$ 이거나 $m \in \{5 \sim 18,\ 30,\ 42,\ 46,\ 48 \sim 50,\ 54 \sim 57\}$ 인 경우 GBTD$(5,\ m)$ 이 존재한다.[4] n 이 홀씨수의 제곱일 때 GBTD$(n,\ n)$ 이 존재한다.[4, 5]

GBTD의 구성방법들을 보면 아핀면, HGBTD, FGDRP와 같은 보조적인 배치를 리용하는 방법[3, 4, 6], 차분행렬(DM)을 리용하여 구성하는 방법[4], k 가 홀씨수의 제곱일 때와 동등한 k^2 차행렬의 구성에 의한 방법[5] 등이 있다.

우리는 론문에서 다음의 표기들을 리용한다.

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

$\mathbf{F}_n$ 은 원소수가 n 인 유한체이다.

우리의 결과는 다음의 세가지 보조정리에 기초하고있다.

보조정리 2[4] 위수가 k 인 가법군우에서의 균일한 $(k,\ k,\ k-1)-$DM 이 존재하면 $G \times \mathbf{Z}_k$ 우에서의 GBTD$(k,\ k)$ 가 존재한다.

보조정리 3 균일한 $(4,\ 4,\ 3)-$DM 이 존재한다.

증명 G 를 유한체 $\mathbf{F}_4 = \mathbf{Z}_2[x]/(x^2+x+1) = \{0,\ 1,\ x,\ x+1\}$ 의 가법군으로 취한다.

$\mathbf{F}_4$ 우에서 4차행렬 $D_1,\ D_2,\ D_3$ 을

$$D_i = \begin{pmatrix} y \\ xy \\ (x+1)y + a_i \\ b_i \end{pmatrix},\ i = \overline{1,\ 3}$$

과 같이 구성한다. 여기서 $y \in \mathbf{F}_4$ 이고 $a_1 = 0,\ a_2 = 1,\ a_3 = x$ 이며 $b_i \in \mathbf{F}_4,\ i = \overline{1,\ 3}$ 이다. 그리고 b_i 들은 서로 다르다. 마지막 행벡토르는 모든 성분들이 b_i 이다.

매 D_i 에 대하여 D_i 의 임의의 서로 다른 두 행의 차가 $\mathbf{F}_4$ 의 원소들을 꼭 한번씩 포함한다는것은 쉽게 알수 있다. 따라서 행렬 $D^* = (D_1 \mid D_2 \mid D_3)$ 역시 차분행렬이다.

그런데 D^* 에서 첫 3개의 행들에는 모든 원소들이 다 3번씩 포함되지만 마지막행에는 $b_1,\ b_2,\ b_3$ 들이 각각 4번씩 포함된다. 즉 균일하지 않다.

D^* 을 균일하게 변경시키기 위한 한가지 해결방도는 매 D_i 의 마지막행들에서 각각 하나의 원소를 $b_1,\ b_2,\ b_3$ 이 아닌 $\mathbf{F}_4$ 의 나머지원소 즉 $\Sigma = b_1 + b_2 + b_3$ 으로 바꾸면서도 여전히 차분행렬이 되도록 하는것이다.

$i = \overline{1,\ 3}$ 에 대하여 매 D_i 에서 마지막행의 j_i 번째 원소들을 Σ 로 교체한다고 하자.

이때 교체전과 교체후의 원소들만을 추려서 보면 다음과 같다.(표 1, 2)

표 1. 교체전의 원소들

j_1	j_2	j_3
$x\ j_1$	$x\ j_2$	$x\ j_3$
$(x+1)\ j_1$	$(x+1)\ j_2 + 1$	$(x+1)\ j_3 + x$
b_1	b_2	b_3

표 2. 교체후의 원소들

j_1	j_2	j_3
$x\ j_1$	$x\ j_2$	$x\ j_3$
$(x+1)\ j_1$	$(x+1)\ j_2 + 1$	$(x+1)\ j_3 + x$
Σ	Σ	Σ

교체전의 행렬에서 임의의 서로 다른 두 행의 차가 $\mathbf{F}_4$ 의 원소들을 꼭 세번씩 포함하므로

$$\begin{cases}\{j_1+b_1,\ j_2+b_2,\ j_3+b_3\}=\{j_1+\Sigma,\ j_2+\Sigma,\ j_3+\Sigma\}\\ \{xj_1+b_1,\ xj_2+b_2,\ xj_3+b_3\}=\{xj_1+\Sigma,\ xj_2+\Sigma,\ xj_3+\Sigma\}\\ \{(x+1)j_1+b_1,\ (x+1)j_2+1+b_2,\ (x+1)j_3+x+b_3\}\\ \qquad =\{(x+1)j_1+\Sigma,\ (x+1)j_2+1+\Sigma,\ (x+1)j_3+x+\Sigma\}\end{cases}$$

이도록 한다.

우리는 $\mathbf{Z}_2$에 기초한 연산을 생각하기때문에 $+$와 $-$는 동등하다고 본다.

이때 우의 련립방정식의 풀이는 총 32개이다.

그러므로 균일한 $(4,\ 4,\ 3)-\mathrm{DM}$이 존재한다.

실례로 방정식의 한 풀이 $b_1=1,\ b_2=x,\ b_3=0,\ j_1=0,\ j_2=1,\ j_3=x$를 리용하여 균일한 $(4,\ 4,\ 3)-\mathrm{DM}$을 만들면 다음과 같다.

0	1	x	$x+1$	0	1	x	$x+1$	0	1	x	$x+1$
0	x	$x+1$	1	0	x	$x+1$	1	0	x	$x+1$	1
0	$x+1$	1	x	1	x	0	$x+1$	x	1	$x+1$	0
$x+1$	1	1	1	x	$x+1$	x	x	0	0	$x+1$	0

따라서 보조정리가 증명된다.(증명끝)

보조정리 3과 같은 방법으로 다음의 사실을 증명할수 있다.

보조정리 4 균일한 $(8,\ 8,\ 7)-\mathrm{DM}$이 존재한다.

보조정리 2−4로부터 다음의 결과가 곧 나온다.

정리 GBTD(4, 4)와 GBTD(8, 8)이 존재한다.

참 고 문 헌

[1] C. J. Colbourn et al.; The CRC Handbook of Combinatorial Designs, CRC Press, 72～336, 2007.
[2] D. R. Stinson; Combinatorial Designs, Springer, 1～108, 2004.
[3] J. X. Yin et al.; Des. Codes Cryptogr., 46, 211, 2008.
[4] P. P. Dai et al.; Des. Codes Cryptogr., 74, 15, 2015.
[5] S. C. Kim et al.; arXiv:1208.1920v1 [math. CO] 9, 2012.
[6] Y. M. Chee et al.; Electron. J. Comb., 20, 2, 2013.

주체108(2019)년 3월 15일 원고접수

Construction of Generalized Balanced Tournament Designs using Difference Matrices

Kim Song Chol

We construct a GBTD(4, 4) and a GBTD(8, 8) using difference matrices.

Key words: generalized balanced tournament design(GBTD), difference matrix