Some existence of perpendicular multi-arrays

Kazuki Matsubara

Chuo Gakuin University

(joint work with Sanpei Kageyama)

2018.5.20-24
JCCA2018
Sendai International Center

BIB design, Perpemdicular array

- V is a finite set, $|V| = v$.
- $\mathcal{B} = \{B_j \mid 1 \leq j \leq b\}, B_j = \{v_{jh} \mid 1 \leq h \leq k\}$.

  Elements of V are called "points"
  Elements of $\mathcal{B}$ are called "blocks"

Balanced incomplete block design $(V, \mathcal{B})$, (v, k, λ)-BIBD

- Every pair of points $x, y \in V$ occurs in exactly λ blocks, i.e.,
  $$|\{B_j \mid \{x, y\} \subset B_j\}| = \lambda.$$

Perpendicular array $A = (v_{jh})$, $b \times k$ array, $\mathrm{PA}_\lambda(k, v)$

- Each row has k distinct points.
- Every set of two columns contains each pair of distinct points $x, y \in V$ as a row precisely λ times, i.e.,
  $$|\{j \mid x = v_{jh_1}, y = v_{jh_2} \text{ or } y = v_{jh_1}, x = v_{jh_2}\}| = \lambda,$$
  for any h_1, h_2 with $1 \leq h_1 < h_2 \leq k$.

Splitting type of combinatorial structures

- V is a finite set, $|V| = v$.
- $\mathcal{B}^* = \{B_j^* \mid 1 \le j \le b\}, B_j^* = \bigcup_{1 \le h \le k} B_{jh}$, $|B_{jh}| = c$.

  Elements of V are called "points"
  Elements of $\mathcal{B}^*$ are called "super-blocks"
  B_{jh}'s are called "sub-blocks"

Splitting-balanced block design $(V, \mathcal{B}^*)$, $(v, k \times c, \lambda)$-SBD

- Every pair of points $x, y \in V$ occurs in exactly λ super-blocks such that x and y are in "different" sub-blocks, i.e.,
$$|\{B_j^* \mid x \in B_{jh_1}, y \in B_{jh_2}, h_1 \ne h_2\}| = \lambda.$$

Perpendicular multi-array $A = (B_{jh})$, $\mathrm{PMA}_\lambda(k \times c, v)$

- In each row, $B_{jh_1} \cap B_{jh_2} = \phi$ $(h_1 \ne h_2)$.
- For any h_1, h_2 with $1 \le h_1 < h_2 \le k$ and any $x, y \in V$,
$$|\{j \mid x \in B_{jh_1}, y \in B_{jh_2} \text{ or } y \in B_{jh_1}, x \in B_{jh_2}\}| = \lambda.$$

Examples

Cyclic $\mathsf{PMA}_1(2 \times 2, 9)$

$$\begin{pmatrix} \color{red}{0,1} & | & \color{red}{2,4} \\ 1,2 & | & 3,5 \\ 2,3 & | & 4,6 \\ 3,4 & | & 5,7 \\ 4,5 & | & 6,8 \\ 5,6 & | & 7,0 \\ 6,7 & | & 8,1 \\ 7,8 & | & 0,2 \\ 8,0 & | & 1,3 \end{pmatrix}$$

Cyclic $\mathsf{PMA}_1(3 \times 2, 17)$

$$\begin{pmatrix} \color{red}{0,13} & | & \color{red}{3,9} & | & \color{red}{2,12} \\ 1,14 & | & 4,10 & | & 3,13 \\ 2,15 & | & 5,11 & | & 4,14 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 16,12 & | & 2,8 & | & 1,11 \\ \color{red}{0,16} & | & \color{red}{1,11} & | & \color{red}{7,13} \\ 1,0 & | & 2,12 & | & 8,14 \\ 2,1 & | & 3,13 & | & 9,15 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 16,15 & | & 0,10 & | & 6,12 \end{pmatrix}$$

Red : Base blocks on $\mathbb{Z}_v$

Difference method

Perpendicular difference multi-array $D = (B_{jh})$, PDMA$_\lambda(k \times c, v)$

- For any h_1, h_2 with $1 \le h_1 < h_2 \le k$,

$$\bigcup_{\substack{d_j \in B_{jh_1}, d'_j \in B_{jh_2} \\ 1 \le j \le \lambda(v-1)/(2c^2)}} \{\pm(d_j - d'_j)\} = \lambda(\mathbb{Z}_v \setminus \{0\}).$$

.

- PDMA$_1(3 \times 2, 17)$:

$$\left(\begin{array}{c|c|c} 0, 13 & 3, 9 & 2, 12 \\ 0, 16 & 1, 11 & 7, 13 \end{array}\right)$$

Lemma 1

The existence of a PDMA$_\lambda(k \times c, v)$ implies the existence of a cyclic PMA$_\lambda(k \times c, v)$.

Authentication perpendicular multi-array

M. Li, M. Liang, B. Du and J. Chen,
A construction for optimal c-splitting authentication and secrecy codes,
Des. Codes Cryptogr., 2017, published online.

Additional property for the authentication PMA

- For any $x, y \in V$, we have that among all the rows of A which contain x, y in different columns, the x occurs in all columns equally often.

Theorem 2 (Li et al, 2017)

There exists an authentication $\text{PMA}_1(3 \times 2, v)$ if and only if $v \equiv 1 \pmod 8$ with seven possible exceptions $v \in \{9, 17, 41, 65, 113, 161, 185\}$.

Necessary conditions

For the existence of a $(v, k \times c, \lambda)$-SBD

- If there exists a $(v, k \times c, \lambda)$-SBD, then

$$b = \frac{\lambda v(v-1)}{c^2 k(k-1)}, \ r = \frac{\lambda(v-1)}{c(k-1)}, \tag{1}$$

$$b \geq \frac{v-1}{k-1}. \tag{2}$$

For the existence of a PMA$_\lambda(k \times c, \lambda)$

- If there exists a PMA$_\lambda(k \times c, v)$, then

$$b = \frac{\lambda v(v-1)}{2c^2}, \ r = \frac{\lambda k(v-1)}{2c}, \tag{3}$$

$$b \geq v-1. \tag{4}$$

$\mathrm{PMA}_\lambda(2 \times c, v)$

$\mathrm{PMA}_\lambda(2 \times c, v)$ with $b \geq v-1$

- $\mathrm{PMA}_\lambda(2 \times c, v) \iff (v, 2 \times c, \lambda)$-SBD

$\mathrm{PMA}_\lambda(2 \times c, v)$ with $b = v-1$

- $\mathrm{PMA}_\lambda(2 \times c, v) \iff (2c, 2 \times c, c)$-SBD
  $\iff$ Hadamard matrix of order 2c

$\mathrm{PMA}_\lambda(2 \times c, v)$ with $b = v$

- $\mathrm{PMA}_1(2 \times c, 2c^2+1)$ and $\mathrm{PMA}_2(2 \times c, c^2+1)$ for any $c \geq 2$
- Near-resolvable $(2c+1, c, tc)$-BIBD $\iff \mathrm{PMA}_{t(c-1)}(2 \times c, 2c+1)$

Theorem 3

- When $c \geq 3$ and $t \geq 1$ are both odd, no $\mathrm{PMA}_{tc}(2 \times c, 2c)$ exists.
- For even c, a $\mathrm{PMA}_c(2 \times c, 2c+1)$ exists only if $2c+1$ is the sum of two squares.

$\mathrm{PMA}_\lambda(3 \times c, v)$

Necessary condition for the case of $k \geq 3$

$$b = \frac{\lambda v(v-1)}{2c^2}, \; r' = \frac{\lambda(v-1)}{2c}, \tag{5}$$

$$b \geq v. \tag{6}$$

Question

Are there $\mathrm{PMA}_\lambda(k \times c, v)$ with $k \geq 3$ and $b = v$?

Question

Are the conditions (3) and (4) (or (5) and (6)) sufficient for the existence of a $\mathrm{PMA}_\lambda(k \times c, v)$ (with $k \geq 3$)?

Lemma 4

There is no $\mathrm{PMA}_1(3 \times 2, 9)$.

$\mathrm{PMA}_\lambda(3 \times 2, v)$

- $\lambda \equiv 1, 3 \pmod 4 \implies v \equiv 1 \pmod 8$
- $\lambda \equiv 2 \pmod 4 \implies v \equiv 1 \pmod 4$
- $\lambda \equiv 0 \pmod 4 \implies$ any v

Lemma 5

There exists a $\mathrm{PMA}_4(3 \times 2, v)$ for any $v \geq 6$.

※ The $\mathrm{PMA}_4(3 \times 2, v)$ for any $v \geq 6$ has been obtained as 3-pairwise additive BIB designs in the literature.

Remaining cases

- $v = 17, 41, 65, 113, 161, 185$ with $\lambda = 1$
- $v \equiv 5 \pmod 8$ with $\lambda = 2$

SBD construction

Lemma 6

The existence of a $(v, k \times c, \lambda)$-SBD and a $\mathrm{PA}_1(k, k)$ implies the existence of a $\mathrm{PMA}_\lambda(k \times c, v)$.

Known results:

The necessary conditions (1) and (2) are also sufficient for the existence of a $(v, k \times c, \lambda)$-SBD when

- $(k, c) = (2, 3)$ with the definite exception of $v = 6$ and $\lambda \equiv 3 \pmod 6$
- $(k, c) = (2, 5)$ with the possible exception of $v = 76$
- $(k, c) = (3, 2)$
- $\cdots$

GDD construction

- V is a finite set, $|V| = v$.
- $\mathcal{G}$ is a partition of V into subsets (called groups).
- $\mathcal{B} = \{B_j \mid 1 \le j \le b\}, B_j = \{v_{jh} \mid 1 \le h \le k\}$, $|\mathcal{B}| = b$.

Group Divisible Design $(V, \mathcal{G}, \mathcal{B})$, (v, k, λ)-GDD

- Each block intersects any given group in at most one point.
- Each $x, y \in V$ from distinct groups is contained in exactly λ blocks.

PMA from GDD

$(12t + 8, 3, 1)$-GDD of type $12^t 8$

$$\left.\begin{array}{l} \text{PMA}_1(3 \times 2, 25) \\ \text{PMA}_1(3 \times 2, 17) \end{array}\right. \implies \text{PMA}_1(3 \times 2, 25t + 17)$$

Lemma 7

There exists a $\text{PMA}_1(3 \times 2, 25t + 17)$ for any $t \ge 3$.

Case of $\lambda = 1$

Lemma 8

There exists a $\text{PMA}_1(3 \times 2, v)$ if and only if $v \equiv 1 \pmod 8$ with the definite exception of $v = 9$.

- For $v \notin \{9, 17, 41, 65, 113, 161, 185\}$: Theorem 2
- For $v = 9$: non-existence by Lemma 4
- For $v = 17, 41$: individual examples of PDMAs

$$\begin{pmatrix} 0,24 & | & 1,15 & | & 33,36 \\ 0,21 & | & 28,33 & | & 2,35 \\ 0,27 & | & 3,25 & | & 17,20 \\ 0,1 & | & 22,37 & | & 26,28 \\ 0,17 & | & 11,27 & | & 30,40 \end{pmatrix} \text{ mod } 41$$

- For $v = 113, 161, 185$: Lemma 7
- For $v = 65$: from a $(32, 3, 1)$-GDD of type 8^4

Case of $\lambda = 2$

Lemma 9

There exists a $\mathrm{PMA}_2(3 \times 2, v)$ if and only if $v \equiv 1 \pmod 4$.

- For $v \equiv 1 \pmod 8$: copies of the case of $\lambda = 1$
- For $v = 9, v \equiv 13, 21 \pmod{24}$: from a $(v, 3 \times 2, 2)$-SBD
- For $v = 29$: an individual example of a PDMA

$$\begin{pmatrix} 0,5 & | & 1,22 & | & 10,25 \\ 0,23 & | & 3,6 & | & 8,26 \\ 0,28 & | & 1,2 & | & 12,15 \\ 0,28 & | & 18,21 & | & 10,20 \\ 0,13 & | & 4,24 & | & 1,11 \\ 0,28 & | & 5,13 & | & 1,6 \\ 0,2 & | & 15,21 & | & 7,25 \end{pmatrix} \text{ mod } 29$$

- For $v = 24t + 29$ with $t \geq 1$:
  from a $(12t + 14, 3, 1)$-GDD of type $6^{2t+1}8$

Main result

Theorem 10

The necessary condition (5) is also sufficient for the existence of a $\mathrm{PMA}_\lambda(3 \times 2, v)$ with the definite exception of $(v, \lambda) = (9, 1)$.

- Lemmas 5, 8 and 9
- copies of the case of $\lambda = 1, 2, 4$
- a $\mathrm{PMA}_3(3 \times 2, 9)$

Corollary 11

There exists no authentication $\mathrm{PMA}_1(3 \times 2, 9)$.

Future works

- Constructions of a PMA$_\lambda(4 \times 2, v)$
- Characterizations of the PMA$_\lambda(k \times c, v)$ with $b = v$
- The existence of a cyclic (or 1-rotational) PMA$_\lambda(k \times c, v)$
- The existence of arrays allowed various sizes of sub-blocks

Example 12

PMA$_2(3 \times 6, 37)$:

$$(0, 13, 15, 17, 20, 35 \mid 3, 5, 11, 19, 28, 34 \mid 9, 14, 22, 27, 32, 33) \mod 37.$$

Future works

- Constructions of a $\mathrm{PMA}_\lambda(4 \times 2, v)$
- Characterizations of the $\mathrm{PMA}_\lambda(k \times c, v)$ with $b = v$
- The existence of a cyclic (or 1-rotational) $\mathrm{PMA}_\lambda(k \times c, v)$
- The existence of arrays allowed various sizes of sub-blocks

Example 12

$\mathrm{PMA}_2(3 \times 6, 37)$:

$$(0, 13, 15, 17, 20, 35 \mid 3, 5, 11, 19, 28, 34 \mid 9, 14, 22, 27, 32, 33) \mod 37.$$

Thank you for your attention