

Lecture 10

May, 30, 2024

Disproof of Euler's Conjecture

Definition (Transversal Designs)

$(X, \mathcal{B})$,

An $\text{GDD}(n, m; m, \lambda)$, is also known as a transversal design

$T(n; m, \lambda)$, i.e., each block is of size m (the number of blocks or each block $B \in \mathcal{B}$ intersects each group.

Observation

The existence of a pair of orthogonal Latin squares of order n is equivalent to the existence of a $T(n; 4, 1)$ design.

(*) If we can construct a $T(n; m, 1)$, then there exist $m-2$ $\text{MOLS}(n)$'s.

(•) Since a $T(n; n+1, 1)$ exists for prime power n , there exist $n-1$ $\text{MOLS}(n)$'s.

(*) A consequence of $\text{PG}(n)$: Delete an element say "0" and then keep all the blocks of size $n+1$.

2

Another idea of constructing $\text{MOLS}(n)$'s comes from the construction of $\text{PBD}, (X, B)$, where $|X| = n$.

(*) Theorem Let (X, B) be λ - $(n, K, 1)$ design such that for each $k \in K$, there exist at least t mutually orthogonal Latin squares of order k . Then, there exist $t-1$ $\text{MOLS}(n)$'s.

Proof If for each $k \in K$, there exists an idempotent Latin square of order k , then there exists an idempotent $\text{LS}(n)$ which is obtained from (X, B) , see next page for an example.

Therefore, if there are at least $t-1$ ^{idempotent} mutually orthogonal Latin squares of order k for each $k \in K$, then we can

construct $t-1$ idempotent Latin squares of order n .

(*) (A consequence of the existence of t $\text{MOLS}(k)$'s.)

By the fact that all induced subsquares from blocks are orthogonal, these $t-1$ Latin squares of order n are also mutually orthogonal.

(By two finger's rule!?)

Exercise 5-2 prove that if there exist three $\text{MOLS}(k)$'s, then there exist two $\text{MOLS}(k)$'s L and M such that L and M are idempotent $\text{LS}(k)$'s. (3 points) (See 3' for an example.) Per-Due

$$X = \{0, 1, 2, \dots, 9\}$$

$$B = \{0123, 0456, 0789, 147, 258, 369, 159, 267, 348, 168, 249, 357\}$$

(X, B) is a $2-(10, \{3, 4\}, 1)$ design.

L:

0	2	3	1	5	6	4	8	9	7
3	△	0	2	△	9	8	△	6	5
1	3	2	0	9	8	7	6	5	4
2	0	1	3	8	7	9	5	4	6
6	△	9	8	△	0	5	△	3	2
4	9	8	7	6	5	0	3	2	1
5	8	7	9	0	4	6	2	1	3
9	△	6	5	△	3	2	△	0	8
7	6	5	4	3	5	1	9	8	0
8	5	4	6	2	1	3	0	△	9

a	c	b
c	b	a
b	a	c

a	c	d	b
d	b	a	c
b	d	c	a
c	a	b	d

(x) If $\{i, j\}$ occurs in B_k , then use the idempotent

Latin square defined on B_k to fill in L_{ij} or L_{ji} respectively.

Conclusion (i) If $i = j$, then $L_{ij} = i$.

(ii) If $i \neq j$, L_{ij} is an element of B_k where $\{i, j\} \subseteq B_k$.

(iii) $L_{ij} \neq L_{ij'}$ and $L_{ij} \neq L_{i'j}$.

($\{i, j\}$ and $\{i, j'\}$, resp. $\{i, j\}$ and $\{i', j\}$ are not in the same block.)

Example Three MOLS(4)'s

⇒ Two [↑]MOLS(4)'s
idempotent

2	3	0	1
0	1	2	3
3	2	1	0
1	0	3	2

1	0	3	2
0	1	2	3
2	3	0	1
3	2	1	0

3	2	1	0
0	1	2	3
1	0	3	2
2	3	0	1

↓
Diagonal

0	1	2	3
2	3	0	1
3	2	1	0
1	0	3	2

↓ Unipotent

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

↓
Diagonal

0	1	2	3
3	2	1	0
1	0	3	2
2	3	0	1

0	2	3	1
3	1	0	2
1	3	2	0
2	0	1	3

0	3	1	2
2	1	3	0
3	0	2	1
1	2	0	3

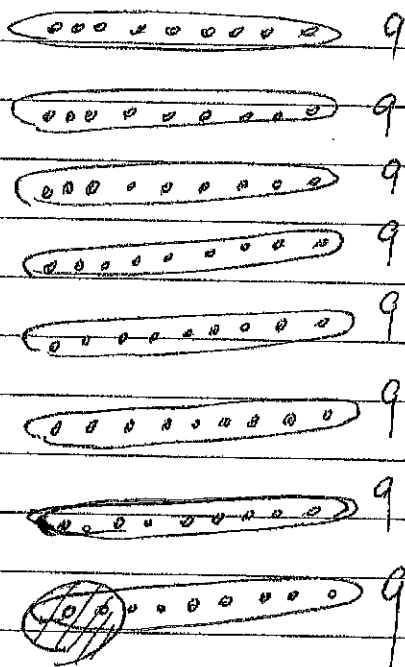
↖ ↗
Idempotent

Since a $2-(22, \{4, 7\}, 1)$ design exists, there exists a pair of $\text{MOLS}(22)$'s. In fact, for each $v \geq 19$ and $v \equiv 1 \pmod{3}$, a $2-(v, \{4, 7\}, 1)$ design exists. (A beautiful work!)

Hence, a pair of $\text{MOLS}(v)$'s exists for $v \equiv 1 \pmod{3}$ and $v \geq 19$.

(*) We can use a $2-(v, \{7, 8, 9\}, 1)$ design exists for certain v 's to show that five $\text{MOLS}(v)$'s exist.

For example, $(v=70)$

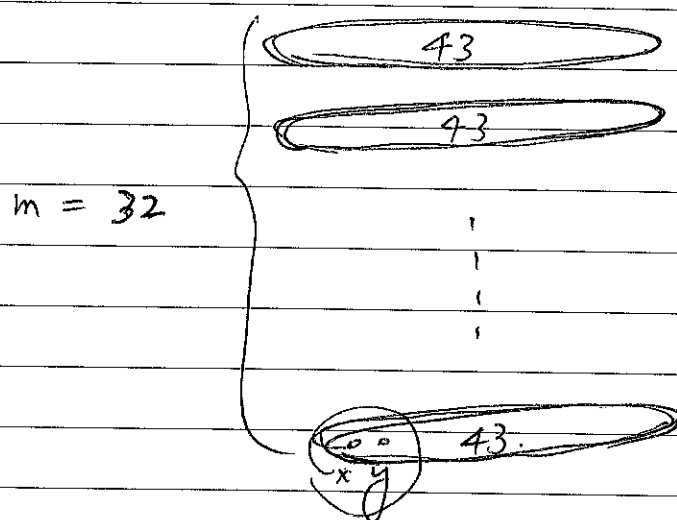


Start with $\text{AG}(9)$ and truncate two elements from the last block.

m is as small as possible and

Exercise 5-3 Find an order $v = 2 \cdot (2m+1)$ such that there exist, at least 7 $\text{MOLS}(v)$'s. (3 points)

See 4' for an example.



$T(43; 32, 1)$ (By using 30 MOLS(43)'s.)
 $\swarrow$
 (X, B)

去掉 x, y ,

$(X \setminus \{x, y\}, B')$ is a $2 - (43 \times 32 - 2, \{31, 32, \overset{41}{43}\}, 1)$

PBD.

$\Rightarrow$ 至少可以找到 29 个互相垂直的 MOLS(1374)'s.

$$(1374 \equiv 2 \pmod{4})$$

(*) P.S. please find another example.

A different approach

Construction of $T(3m+u; 4, 1)$ where

(1) a $T(m; 5, 1)$ exists, (2) a $T(u; 4, 1)$ exists and (3) $m \geq u$.

Step 1 Let (X_1, B_1) be a $T(m; 5, 1)$ with five groups

G_1, G_2, G_3, G_4, G_5 and (X_2, B_2) be a $T(u; 4, 1)$ with

four groups $H_i = \{x_1, x_2, x_3, \dots, x_u\} \times \{i\}$, $i = 1, 2, 3, 4$, i.e.,

$H_i = \{(x_1, i), (x_2, i), \dots, (x_u, i)\} =_{\text{def}} \{x_{1,i}, x_{2,i}, \dots, x_{u,i}\}$.

Step 2 Let (X'_1, B'_1) be the $T(m; 4, 1)$ obtained by truncating

G_5 . Hence, B'_1 can be partitioned into m parallel

classes $L_1, L_2, \dots, L_u, \dots, L_m$ where each L_j is a

set of m disjoint blocks of size 4 defined on

$X_1 \setminus G_5 = X'_1$. ($|X'_1| = 4m$, $|B'_1| = m^2$.)

Step 3 Let $\mathcal{X}$ be defined as follows:

$\overline{G}_1: (G_1 \times \{1\}, G_1 \times \{2\}, G_1 \times \{3\}, H_1)$ ← Each group contains $3m+u$ elements.

$\overline{G}_2: (G_2 \times \{1\}, G_2 \times \{2\}, G_2 \times \{3\}, H_2)$

$\overline{G}_3: (G_3 \times \{1\}, G_3 \times \{2\}, G_3 \times \{3\}, H_3)$

$\overline{G}_4: (G_4 \times \{1\}, G_4 \times \{2\}, G_4 \times \{3\}, H_4)$

An example, $m=7, u=5$, (Notation for $T(3m+u; 4, 1)$)

$$G_1 = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7\}$$

$$H_i = \{(x_1, i), (x_2, i), (x_3, i), (x_4, i), (x_5, i)\}$$

$$G_2 = \{g_8, g_9, g_{10}, g_{11}, g_{12}, g_{13}, g_{14}\}$$

$$= \{x_{1,i}, x_{2,i}, x_{3,i}, x_{4,i}, x_{5,i}\}$$

$$G_3 = \{g_{15}, g_{16}, g_{17}, g_{18}, g_{19}, g_{20}, g_{21}\}$$

$$G_j \times \{j\} = \{g_{1,j}, g_{2,j}, g_{3,j}, \dots, g_{7,j}\}, j=1, 2, \dots, 7.$$

$$G_4 = \{g_{22}, g_{23}, g_{24}, g_{25}, g_{26}, g_{27}, g_{28}\}$$

$$\bar{G}_1: (g_{1,1}) g_{2,1} g_{3,1} g_{4,1} g_{5,1} g_{6,1} g_{7,1} (g_{1,2}) g_{2,2} g_{3,2} g_{4,2} g_{5,2} g_{6,2} g_{7,2} (g_{1,3}) g_{2,3} g_{3,3} g_{4,3} g_{5,3} g_{6,3} g_{7,3} \\ (x_{1,1}) x_{2,1} x_{3,1} x_{4,1} x_{5,1}$$

$$\bar{G}_2: (g_{8,1}) g_{9,1} g_{10,1} g_{11,1} g_{12,1} g_{13,1} g_{14,1} (g_{8,2}) g_{9,2} g_{10,2} \dots g_{14,2} (g_{8,3}) g_{9,3} \dots g_{14,3} (x_{1,2}) x_{2,2} x_{3,2} x_{4,2} x_{5,2}$$

$$\bar{G}_3: (g_{15,1}) g_{16,1} \dots g_{21,1} g_{15,2} g_{16,2} \dots (g_{15,3}) g_{16,3} \dots (g_{15,3}) (x_{1,3}) x_{2,3} x_{3,3} x_{4,3} x_{5,3}$$

$$\bar{G}_4: (g_{22,1}) g_{23,1} \dots g_{28,1} g_{22,2} g_{23,2} \dots (g_{28,2}) g_{22,3} g_{23,3} \dots (g_{28,3}) (x_{1,4}) x_{2,4} x_{3,4} x_{4,4} x_{5,4}$$

In general, $\bar{G}_j = G_j \times \{1, 2, 3\} \cup H_j, j=1, 2, 3, 4$.

Therefore, $X = \bigcup_{j=1}^4 \bar{G}_j$.

The construction follows by defining B properly!

(in next page)

7

Step 4 Choose u parallel classes from (X', B') , say
 (There are m parallel classes in B')

$L_1, L_2, \dots, L_u$. Starting from $L_1 = \{B_{1,1}, B_{2,1}, \dots, B_{m,1}\}$, use

$(B_{i,1} \times \{1, 2, 3\}) \cup \{x_{i,1}, x_{i,2}, x_{i,3}, x_{i,4}\}$ to construct a $T(4; 4, 1)$ which

contains the block $\{x_{i,1}, x_{i,2}, x_{i,3}, x_{i,4}\}$. $\rightarrow$ 这个 block 固定, 但是 i

是由 1 到 m , 因此我们有 m 个 $T(4; 4, 1)$. 一直到 L_u 固定,

$\{x_{u,1}, x_{u,2}, x_{u,3}, x_{u,4}\}$. (对于每个固定的 u , 一共有 $15mu$ 个 blocks.)

$B' = \{a, b, c, d\}$

Step 5 For those blocks in $L_{u+1} \cup L_{u+2} \cup \dots \cup L_m$, we use

$\begin{cases} (a, 1), (a, 2), (a, 3) \\ (b, 1), (b, 2), (b, 3) \\ (c, 1), (c, 2), (c, 3) \\ (d, 1), (d, 2), (d, 3) \end{cases}$ to construct a $T(3; 4, 1)$.
 (9 blocks)

In total, we have $9 \cdot (m-u)m$ blocks.

Step 6 Construct a $T(u; 4, 1)$ based on $\bigcup_{j=1}^u H_j$.

In total, we have u^2 blocks. Combining Steps 4-6, we

have $15mu + 9m^2 - 9um + u^2 = 9m^2 + 6mu + u^2 = (3m+u)^2$.

Step 7 Step 6 shows that the total number of pairs we have
 (from different groups)

is $6 \cdot (3m+u)^2$. We have to claim every pair from different groups
 occurs in a block in Steps 4-6.

Now, consider (y, i) and (z, j) , $i \neq j$. If one of them is equal to x , then they occur together in a block ^(y and z) either from Step 4 or Step 6. On the other hand, both of them are not equal to x , then they occur together in a block ^(y and z) of (X', B') _{$1 \leq i+j \leq 3$} . Hence, they, (y, i) and (z, j) , occur together in blocks from Step 4 or 5 depending on whether y and z are in a block of the u parallel classes or not.

⊗ Theorem A. If there exist three MOLS(m)s and two MOLS(u)'s, then there exists a pair of MOLS($3m+u$).

(**) Choose prime powers m and $u \neq 2$ or 6 to construct the
(Idea) desired MOLS($3m+u$).

$$(m, u) \Rightarrow (5, 3) \rightarrow 18$$

$$(7, 1) \rightarrow 22$$

$$(7, 5) \rightarrow 26$$

$$(9, 3) \rightarrow 30$$

$$(9, 7) \rightarrow 34$$

⋮

⋮

⋮

10 和 14 需要独立建構, 無法使用上述 Theorem A. ^{Per-Duo}

n	m	u
$18k$	$6k-1$	3
$18k+2$	$6k-1$	5
$18k+4$	$6k+1$	1
$18k+6$	$6k+1$	3
$18k+8$	$6k+1$	5
$18k+10$	$6k+1$	7
$18k+12$	$6k+1$	9
$18k+14$	$6k+1$	11
$18k+16$	$6k+5$	1

n, m, u 的選擇

← $k \geq 2$; the case $k=1$ can be replaced by letting $m=9$ and $u=3$.

$(6k+1, 13)$ 在 $k=1$ 時不能用.

Exercise 5-4 (3 points)

Apply Theorem A to prove that

there exists a pair of MOLS(v)'s for each $v \in$

$\{1, 2, 6\}$.

较早发现

以下是互相垂直的兩個 10 階拉丁方陣，E.T.Park 與 Bose 及 Shrikhande 在 1959 年分別宣稱推翻了尤拉猜測，然而 Bose 及 Shrikhande 兩人的工作似乎獲得較明確的肯定，這應該歸功於他們完整的工作，也就是對於所有的 $n \equiv 2 \pmod{4}$ ， $n \geq 10$ ，都能建構 2 個 $\text{MOLS}(n)$ ，而不是只有 10 階拉丁方陣。

4	0	9	8	3	2	7	5	6	1
2	3	7	5	4	0	9	8	1	6
8	1	6	9	0	4	5	3	2	7
9	8	1	4	5	6	3	2	7	0
0	9	8	6	1	3	2	7	4	5
7	2	3	1	6	5	4	0	9	8
5	4	0	3	2	7	6	1	8	9
6	5	4	2	7	1	8	9	0	3
1	6	5	7	8	9	0	4	3	2
3	7	2	0	9	8	1	6	5	4

5	4	0	1	2	7	8	9	3	6
3	1	6	4	8	5	9	2	0	7
0	9	8	7	3	6	1	4	5	2
2	5	4	3	6	1	7	8	9	0
9	8	7	6	1	0	4	5	2	3
1	6	3	5	9	2	0	7	4	8
8	7	2	9	0	4	5	3	6	1
4	0	9	2	7	8	3	6	1	5
7	2	5	0	4	3	6	1	8	9
6	3	1	8	5	9	2	0	7	4

兩個互相垂直的 10 階拉丁方陣

定理 4.11. 對於所有的 n ，除了 1, 2, 6 之外， $M(n) \geq 2$ 。

證明： $n \equiv 2 \pmod{4}$ 留在第三章證明。

垂直拉丁方陣需要利用組合設計來協助建構，而反過來，我們也可以利用它來建構組合設計，參考第二章。另一方面，在實驗設計上，它也扮演非常重要的角色。下頁是 $\text{MOLS}(14)$ 。

12	7	0	6	4	2	11	9	13	5	3	1	10	8
1	11	10	4	5	6	13	8	9	0	7	12	2	3
2	1	11	0	7	12	3	4	5	6	13	8	9	10
10	9	8	1	2	3	4	5	6	13	0	7	12	11
7	0	12	3	1	10	8	6	4	2	11	9	13	5
3	2	1	13	8	9	10	11	0	7	12	4	5	6
5	4	3	10	11	1	2	0	7	12	6	13	8	9
13	6	5	2	3	4	0	7	12	8	9	10	11	1
9	8	13	5	6	0	7	12	10	11	1	2	3	4
11	10	9	8	0	7	12	1	2	3	4	5	6	13
0	12	7	11	9	13	5	3	1	10	8	6	4	2
4	3	2	7	12	5	6	13	8	9	10	11	1	0
6	5	4	12	13	8	9	10	11	1	2	3	0	7
8	13	6	9	10	11	1	2	3	4	5	0	7	12

12	13	4	10	7	0	1	9	6	3	11	8	5	2
9	8	10	5	6	7	4	13	12	11	1	2	3	0
5	0	6	7	8	9	10	11	1	2	3	4	13	12
6	5	7	1	2	3	0	4	13	12	8	9	10	11
4	12	13	6	3	11	8	5	2	10	7	0	1	9
1	11	2	9	10	4	13	12	3	0	5	6	7	8
0	3	5	2	4	13	12	6	7	8	9	10	11	1
7	6	8	4	13	12	9	10	11	1	2	3	0	5
10	9	11	13	12	1	2	3	0	5	6	7	8	4
2	1	3	12	0	5	6	7	8	9	10	11	4	13
13	4	12	3	11	8	5	2	10	7	0	1	9	6
8	7	9	11	1	2	3	0	5	6	4	13	12	10
11	10	1	0	5	6	7	8	9	4	13	12	2	3
3	2	0	8	9	10	11	1	4	13	12	5	6	7

MOLS(14)