

MAGIC SQUARES AND ORTHOGONAL ARRAYS

Donald L. Kreher

Michigan Technological University

3 November 2011 - University of Minnesota-Duluth

REFERENCES

- Andrews, W.S. Magic Squares And Cubes. Dover, (1960).
- Franklin, B., Autobiography of Benjamin Franklin. (Leonard W. Labaree (Editor)) Yale Univ Press, (1964) .
- Hilliard, J.N. Greater Magic. Kaufman and Greenberg, (1994).
- Laywine, C.F. and G.L. Mullen. Discrete Mathematics Using Latin Squares, (1998).
- Lindner, C.C. and C.A. Rodger, Design Theory, CRC press, (1997).
- Rouse Ball, W.W. and H. S. M. Coxeter, Mathematical Recreations and Essays. Dover (1987).

FUNDAMENTALS
OF COMBINATORIAL MATHEMATICS

1. What is combinatorial mathematics? Combinatorial mathematics also referred to as combinatorial analysis or combinatorics, is a mathematical discipline that began in ancient times. According to legend the Chinese Emperor Yu (c. 2200 B.C.) observed the magic square

$$\begin{bmatrix} 4 & 9 & 2 \\ 3 & 5 & 7 \\ 8 & 1 & 6 \end{bmatrix}$$

on the shell of a divine turtle. ...

– H.J. Ryser, *Combinatorial Mathematics*, C.M. 14 (1963).



Definition:

A *magic square* is an n by n array of integers with the property that the sum of the numbers in each row, each column and the the main and back diagonals is the same. This sum is the *magic sum*.

The square is *n -th order* if the integers $1, 2, 3, \dots, n^2$ are used

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

$$n = 4 \quad \text{magic sum} = 34$$

The magic sum of an n -th order magic square is

$$\frac{1}{n} (1 + 2 + \dots + n^2) = \frac{n(n^2 + 1)}{2}$$

THE FRANKLIN SQUARE OF ORDER 8:



"I was at length tired with sitting there to hear debates, in which, as clerk, I could take no part, and which were often so unentertaining that I was induc'd to amuse myself with making *magic squares* or circles, or any thing to avoid weariness; "

Benjamin Franklin Autobiography

52	61	4	13	20	29	36	45
14	3	62	51	46	35	30	19
53	60	5	12	21	28	37	44
11	6	59	54	43	38	27	22
55	58	7	10	23	26	39	42
9	8	57	56	41	40	25	24
50	63	2	15	18	31	34	47
16	1	64	49	48	33	32	17

For what n does an n -th order magic square exist?

Let \mathcal{M} be the set of all positive integers n such that an n -th order magic square exists.

So far we know $3, 4, 8 \in \mathcal{M}$ and it is easy to see that $2 \notin \mathcal{M}$.

SQUARES OF ODD ORDER, DE LA LOUBÉRE (1693)

First place 1 in the middle cell of the first row.

The numbers are placed consecutively $1, 2, 3, \dots, n^2$ in diagonal lines which slope upward to the right except

- 1 When the top row is reached the next number is written in the bottom row as if it were the next row after the top.
- 2 when a right hand column is reached, the next number is written in the left hand column as if it followed the right-hand column;
- 3 if a cell is reached that is already filled or if the upper right corner is reached then the next cell to be used is the one directly below it.

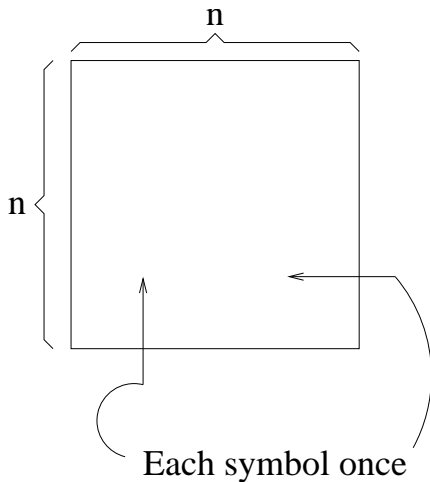
Example

17	24	1	8	15
23	5	7	14	16
4	6	13	20	22
10	12	19	21	3
11	18	25	2	9

This shows that $2m + 1 \in \mathcal{M}$ for all m .

A *Latin square* of order n

- n by n array
- symbols in $\{0, 1, 2, \dots, n - 1\}$
- each row and column contains each symbol

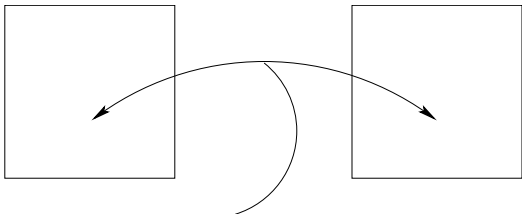


0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

Two Latin squares **A** and **B** of order n are said to be *orthogonal Latin squares* if the n^2 ordered pairs

$$(\mathbf{A}[\mathbf{x}, \mathbf{y}], \mathbf{B}[\mathbf{x}, \mathbf{y}])$$

are all distinct. ($x = 0, 1, 2, 3, \dots, n - 1, y = 0, 1, 2, \dots, n - 1$)



Every ordered pair occurs

0	1	2	3	on	0	1	2	3	is	00	11	22	33
1	0	3	2		2	3	0	1		12	03	30	21
2	3	0	1		3	2	1	0		23	32	01	10
3	2	1	0		1	0	3	2		31	20	13	02

$$M = J + A + 5B$$

Example

$$\begin{array}{rcccl}
 17 & 24 & 1 & 8 & 15 & 1 & 1 & 1 & 1 & 1 & 1 & 3 & 0 & 2 & 4 & 3 & 4 & 0 & 1 & 2 \\
 23 & 5 & 7 & 14 & 16 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 4 & 1 & 3 & 0 & 4 & 0 & 1 & 2 & 3 \\
 4 & 6 & 13 & 20 & 22 & = & 1 & 1 & 1 & 1 & 1 & + & 3 & 0 & 2 & 4 & 1 & +5 & 0 & 1 & 2 & 3 & 4 \\
 10 & 12 & 19 & 21 & 3 & 1 & 1 & 1 & 1 & 1 & 1 & 4 & 1 & 3 & 0 & 2 & 1 & 2 & 3 & 4 & 0 \\
 11 & 18 & 25 & 2 & 9 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 2 & 4 & 1 & 3 & 2 & 3 & 4 & 0 & 1
 \end{array}$$

Better

$$\begin{array}{rcccl}
 18 & 24 & 5 & 6 & 12 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 3 & 4 & 0 & 1 & 3 & 4 & 0 & 1 & 2 \\
 22 & 3 & 9 & 15 & 16 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 2 & 3 & 4 & 0 & 4 & 0 & 1 & 2 & 3 \\
 1 & 7 & 13 & 19 & 25 & = & 1 & 1 & 1 & 1 & 1 & + & 0 & 1 & 2 & 3 & 4 & +5 & 0 & 1 & 2 & 3 & 4 \\
 13 & 11 & 17 & 23 & 4 & 1 & 1 & 1 & 1 & 1 & 1 & 4 & 0 & 1 & 2 & 3 & 1 & 2 & 3 & 4 & 0 \\
 14 & 20 & 21 & 2 & 8 & 1 & 1 & 1 & 1 & 1 & 1 & 3 & 4 & 0 & 1 & 2 & 2 & 3 & 4 & 0 & 1
 \end{array}$$

$$\begin{aligned}
 65 &= (1+1+1+1+1) + (0+1+2+3+4) + 5(0+1+2+3+4) \\
 &\quad (2+2+2+2+2) = (0+1+2+3+4) \\
 &\quad (0+1+2+3+4) = (2+2+2+2+2)
 \end{aligned}$$

Squares of order $2(2m + 1)$ STRACHEY (1918)

Let A be a magic square of order $u = 2m + 1$, $m \geq 1$.

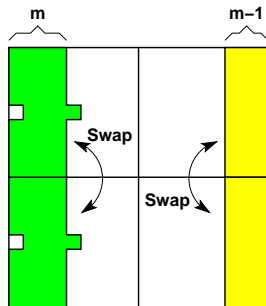
Step 1: Construct this non-magic square of order $2u$:

A	$A+2u^2$
$A+3u^2$	$A+u^2$

Result is a magic square of order $2(2m + 1)$

So $2(2m + 1) = 4m + 2 \in \mathcal{M}$ for all m .

Step 2: Interchange the indicated cells:



Example: $m = 2, u = 5$.

Step 1:

17	24	1	8	15	67	74	51	58	65
23	5	7	14	16	73	55	57	64	66
4	6	13	20	22	54	56	63	70	72
10	12	19	21	3	60	62	69	71	53
11	18	25	2	9	61	68	75	52	59
92	99	76	83	90	42	49	26	33	40
98	80	82	89	91	48	30	32	39	41
79	81	88	95	97	29	31	38	45	47
85	87	94	96	78	35	37	44	46	28
86	93	100	77	84	36	43	50	27	34

Step 2:

92	99	1	8	15	67	74	51	58	40
98	80	7	14	16	73	55	57	64	41
4	81	88	20	22	54	56	63	70	47
85	87	19	21	3	60	62	69	71	28
86	93	25	2	9	61	68	75	52	34
17	24	76	83	90	42	49	26	33	65
23	5	82	89	91	48	30	32	39	66
79	6	13	95	97	29	31	38	45	72
10	12	94	96	78	35	37	44	46	53
11	18	100	77	84	36	43	50	27	59

A magic square of order 10.

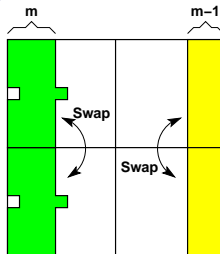
Magic sum=505.

THEOREM. IF $u = 2m + 1 \in \mathcal{M}$, THEN $2u \in \mathcal{M}$.

Proof: Use the Strachey construction.

A	A+2u²
A+3u²	A+u²

Step 1:



Step 2:

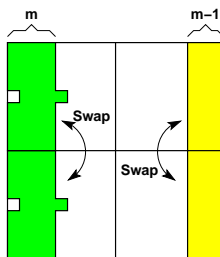
Magic sum of **A** is $\frac{u^3+u}{2}$ In Step 2 we need magic sum $\frac{(2u)^3+2u}{2} = 4u^3 + u$.

THEOREM. IF $u = 2m + 1 \in \mathcal{M}$, THEN $2u \in \mathcal{M}$.

Proof: Use the Strachey construction.

A	$A+2u^2$
$A+3u^2$	$A+u^2$

Step 1:



Step 2:

Magic sum of **A** is $\frac{u^3+u}{2}$ In Step 2 we need magic sum $\frac{(2u)^3+2u}{2} = 4u^3 + u$.

Entries:

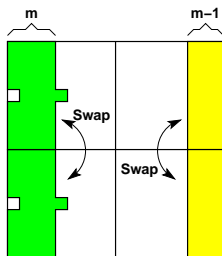
- **Top left** $\{1, 2, 3, \dots, u^2\} + 0u^2 = \{1, 2, 3, \dots, u^2\}$
- **Bottom right** $\{1, 2, 3, \dots, u^2\} + u^2 = \{u^2 + 1, u^2 + 2, u^2 + 3, \dots, 2u^2\}$
- **Top right** $\{1, 2, 3, \dots, u^2\} + 2u^2 = \{2u^2 + 1, 2u^2 + 2, 2u^2 + 3, \dots, 3u^2\}$
- **Bottom left** $\{1, 2, 3, \dots, u^2\} + 3u^2 = \{3u^2 + 1, 3u^2 + 2, 3u^2 + 3, \dots, 4u^2\}$

THEOREM. IF $u = 2m + 1 \in \mathcal{M}$, THEN $2u \in \mathcal{M}$.

Proof: Use the Strachey construction.

A	A+2u²
A+3u²	A+u²

Step 1:



Step 2:

Magic sum of **A** is $\frac{u^3+u}{2}$ In Step 2 we need magic sum $\frac{(2u)^3+2u}{2} = 4u^3 + u$.

Columns: In Step 1 the sum

- of the entries of columns 1 through u is

$$\frac{u^3+u}{2} + \left(\frac{u^3+u}{2} + u \cdot 3u^2\right) = 4u^3 + u$$

- of the entries of columns u through $2u$ is

$$\left(\frac{u^3+u}{2} + u \cdot 2u^2\right) + \left(\frac{u^3+u}{2} + u \cdot u^2\right) = 4u^3 + u$$

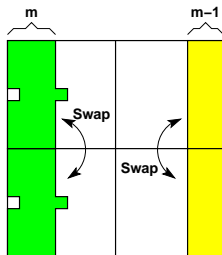
- Step 1 to Step 2 does not change the entries in any column.

THEOREM. IF $u = 2m + 1 \in \mathcal{M}$, THEN $2u \in \mathcal{M}$.

Proof: Use the Strachey construction.

A	A+2u²
A+3u²	A+u²

Step 1:



Step 2:

Magic sum of **A** is $\frac{u^3+u}{2}$ In Step 2 we need magic sum $\frac{(2u)^3+2u}{2} = 4u^3 + u$.

Rows: In Step 2 the sum

- of the entries of rows 1 through u is

$$\left(\frac{u^3+u}{2} + m \cdot 3u^2\right) + \left(\frac{u^3+u}{2} + (m-1) \cdot u^2\right) = 4u^3 + u$$

- of the entries of rows u through $2u$ is

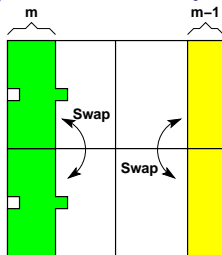
$$\left(\frac{u^3+u}{2} + (m+2) \cdot 3u^2\right) + \left(\frac{u^3+u}{2} + (m+1) \cdot u^2 + (m-1) \cdot 2u^2\right) = 4u^3 + u$$

THEOREM. IF $u = 2m + 1 \in \mathcal{M}$, THEN $2u \in \mathcal{M}$.

Proof: Use the Strachey construction.

A	A+2u²
A+3u²	A+u²

Step 1:



Step 2:

Magic sum of **A** is $\frac{u^3+u}{2}$. In Step 2 we need magic sum $\frac{(2u)^3+2u}{2} = 4u^3 + u$.

Diagonals: In Step 2 the sum

- of the entries on the forward diagonal is

$$\left(\frac{u^3+u}{2} + (m+1) \cdot 3u^2\right) + \left(\frac{u^3+u}{2} + (m+2) \cdot u^2 + (m-1) \cdot 2u^2\right) = 4u^3 + u$$

- of the entries on the backward diagonal is

$$\left(\frac{u^3+u}{2} + m \cdot 3u^2\right) + \left(\frac{u^3+u}{2} + (m+2) \cdot u^2 + (m-1) \cdot 2u^2\right) = 4u^3 + u$$



PRODUCT CONSTRUCTION

Let $A = [a_{ij}]$ be a magic square of order m and magic sum $m(m^2 + 1)/2$.

Let $B = [b_{ij}]$ be a magic square of order n and magic sum $n(n^2 + 1)/2$.

Then the mn by mn square

$$A \otimes B = \begin{bmatrix} (a_{11} - 1)n^2 + B & (a_{12} - 1)n^2 + B & \cdots & (a_{1m} - 1)n^2 + B \\ (a_{21} - 1)n^2 + B & (a_{22} - 1)n^2 + B & \cdots & (a_{2m} - 1)n^2 + B \\ \vdots & & \ddots & \vdots \\ (a_{m1} - 1)n^2 + B & (a_{m2} - 1)n^2 + B & \cdots & (a_{mm} - 1)n^2 + B \end{bmatrix}$$

is a magic square of order mn and magic sum $mn(m^2n^2 + 1)/2$.

Thus: if $m, n \in \mathcal{M}$, then $mn \in \mathcal{M}$.

EXAMPLE:

$$\begin{bmatrix} 8 & 1 & 6 \\ 3 & 5 & 7 \\ 4 & 9 & 2 \end{bmatrix} \otimes \begin{bmatrix} 16 & 3 & 2 & 13 \\ 5 & 10 & 11 & 8 \\ 9 & 6 & 7 & 12 \\ 4 & 15 & 14 & 1 \end{bmatrix} =$$

128	115	114	125	16	3	2	13	96	83	82	93
117	122	123	120	5	10	11	8	85	90	91	88
121	118	119	124	9	6	7	12	89	86	87	92
116	127	126	113	4	15	14	1	84	95	94	81
48	35	34	45	80	67	66	77	112	99	98	109
37	42	43	40	69	74	75	72	101	106	107	104
41	38	39	44	73	70	71	76	105	102	103	108
36	47	46	33	68	79	78	65	100	111	110	97
64	51	50	61	144	131	130	141	32	19	18	29
53	58	59	56	133	138	139	136	21	26	27	24
57	54	55	60	137	134	135	140	25	22	23	28
52	63	62	49	132	143	142	129	20	31	30	17

THEOREM. THERE EXISTS A MAGIC SQUARE OF EVERY ORDER $n \neq 2$

PROOF.

Let \mathcal{M} be the set of n , for which there exists a magic square of order n . We know:

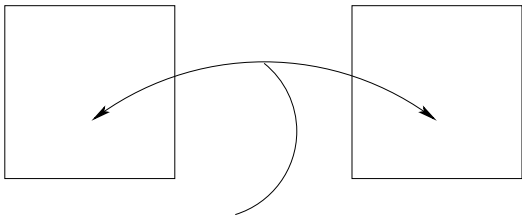
- Ⓐ $1, 3, 4, 8 \in \mathcal{M}$,
 - Ⓑ $2n + 1 \in \mathcal{M}$, for all n ,
 - Ⓒ $4n + 2 \in \mathcal{M}$, for all $n \geq 1$,
 - Ⓓ if $m, n \in \mathcal{M}$, then $mn \in \mathcal{M}$.
- (b) and (c) show that $n \in \mathcal{M}$ for all $n \equiv 1, 2, 3 \pmod{4}$, $n \neq 2$.
 - Use, (a) and (d) to get $4^\ell \in \mathcal{M}$, for all $\ell = 1, 2, 3, \dots$
 - Let $n = 4k = 4^\ell n'$, where $n' \not\equiv 0 \pmod{4}$, $n' > 2$.
 - Then, $n' \in \mathcal{M}$ and $4^\ell \in \mathcal{M}$
 - Use (d) to get $n \in \mathcal{M}$.
 - Therefore $M = \{n \in \mathbb{Z} : n > 0, n \neq 2\}$.



Recall: Two Latin squares **A** and **B** of order n are said to be *orthogonal Latin squares* if the n^2 ordered pairs

$$(\mathbf{A}[x,y], \mathbf{B}[x,y])$$

are all distinct. ($x = 0, 1, 2, 3, \dots, n - 1, y = 0, 1, 2, \dots, n - 1$)



Every ordered pair occurs

0	0 1 2 3	on	0	0 1 2 3	is	0	00 11 22 33
1	1 0 3 2		1	2 3 0 1		1	12 03 30 21
2	2 3 0 1		2	3 2 1 0		2	23 32 01 10
3	3 2 1 0		3	1 0 3 2		3	31 20 13 02

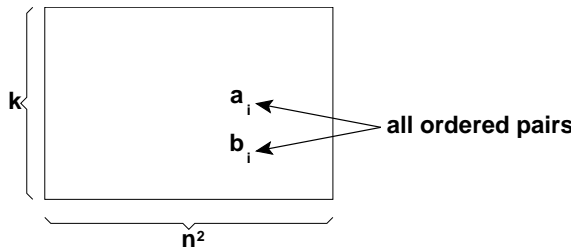
A set of k orthogonal Latin squares A_1, A_2, \dots, A_k are said to be k *mutually orthogonal Latin squares* of order n if they are pairwise orthogonal.

k MOLS(n)

Example: 3 MOLS(4)

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

OA(k, n) ORTHOGONAL ARRAY



Example: OA(3, 3) $\left\{ \begin{array}{l} 0\ 0\ 0\ 1\ 1\ 1\ 2\ 2\ 2 \\ 0\ 1\ 2\ 1\ 2\ 0\ 2\ 0\ 1 \\ 0\ 2\ 1\ 1\ 0\ 2\ 2\ 1\ 0 \end{array} \right.$

Example: OA(5, 4) $\left\{ \begin{array}{l} 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 2\ 2\ 2\ 2\ 3\ 3\ 3\ 3 \\ \mathbf{0\ 1\ 2\ 3\ 0\ 1\ 2\ 3\ 0\ 1\ 2\ 3\ 0\ 1\ 2\ 3} \\ \mathbf{0\ 1\ 2\ 3\ 1\ 0\ 3\ 2\ 2\ 3\ 0\ 1\ 3\ 2\ 1\ 0} \\ \mathbf{0\ 1\ 2\ 3\ 2\ 3\ 0\ 1\ 3\ 2\ 1\ 0\ 1\ 0\ 3\ 2} \\ \mathbf{0\ 1\ 2\ 3\ 3\ 2\ 1\ 0\ 1\ 0\ 3\ 2\ 2\ 3\ 0\ 1} \end{array} \right.$

Theorem: k MOLS(n) is equivalent to an OA($k + 2, n$).

THE PAIR OF ORTHOGONAL LATIN SQUARES TIME LINE.

1782 Euler conjectures that $2 \text{ MOLS}(n)$ exists $\Leftrightarrow n \equiv 0, 1, 3 \pmod{4}$.
He couldn't construct any pair of MOLS of order $2 \pmod{4}$.

1900 G. Tarry In a 33 page paper showed: $\nexists 2 \text{ MOLS}(6)$.

1922 MacNeise conjectures that if $n = p_1^{r_1} p_2^{r_2} \cdots p_x^{r_x}$,
where p_1, p_2, \dots, p_x are distinct primes, then the maximum number of
MOLS(n) is

$$M(n) = \min\{p_1^{r_1}, p_2^{r_2}, \dots, p_x^{r_x}\} - 1$$

1957 E.T. Parker constructs 3 MOLS(21).

This disproves MacNeise's conjecture that the maximum number
would be

$$M(21) = \min\{3, 7\} - 1 = 2.$$

1958 R.S. Bose and S.S. Shrikande construct 2 MOLS(22) disproving
Euler's conjecture. This result made the New York times.

1959 E.T. Parker constructs 2 MOLS(10).

1960 Bose, Shrikande, and Parker proves that there exists 2 MOLS(n) for
every n except for $n = 2$ or $n = 6$ when they cannot exist.

1984 Stinson gives a clever 3 page proof that there do not exist 2 MOLS(6).

THE PAIR OF ORTHOGONAL LATIN SQUARES TIME LINE.

1782 Euler conjectures that 2 MOLS(n) exists $\Leftrightarrow n \equiv 0, 1, 3 \pmod{4}$.

He couldn't construct any pair of MOLS of order $2 \pmod{4}$.

1900 G. Tarry In a 33 page paper showed: \nexists 2 MOLS(6).

1922 MacNeise conjectures that if $n = p_1^{r_1} p_2^{r_2} \cdots p_x^{r_x}$,
where p_1, p_2, \dots, p_x are distinct primes, then the maximum number of
MOLS(n) is

$$M(n) = \min\{p_1^{r_1}, p_2^{r_2}, \dots, p_x^{r_x}\} - 1$$

1957 E.T. Parker constructs 3 MOLS(21).

This disproves MacNeise's conjecture that the maximum number
would be

$$M(21) = \min\{3, 7\} - 1 = 2.$$

1958 R.S. Bose and S.S. Shrikande construct 2 MOLS(22) disproving
Euler's conjecture. This result made the New York times.

1959 E.T. Parker constructs 2 MOLS(10).

1960 Bose, Shrikande, and Parker proves that there exists 2 MOLS(n) for
every n except for $n = 2$ or $n = 6$ when they cannot exist.

1984 Stinson gives a clever 3 page proof that there do not exist 2 MOLS(6).

FINITE FIELD CONSTRUCTION

THEOREM

Let $n = p^\alpha$, where p is a prime and α is a positive integer. Then for $n \geq 3$, there exists $n - 1$ MOLS(n).

PROOF.

Let \mathbb{F}_n be a finite field of order n . For each $f \in \mathbb{F}_n$ define the $\mathbb{F}_n \times \mathbb{F}_n$ matrix A_f by

$$A_f[x, y] = fx + y,$$

for all $x, y \in \mathbb{F}_n$. We claim that the $n - 1$ squares $A_f, f \in \mathbb{F}_q, f \neq 0$ are MOLS(n).

- 1 (Row Latin) If $fx + y_1 = fx + y_2$, then $y_1 = y_2$.
- 2 (Column Latin) If $fx_1 + y = fx_2 + y$, then $fx_1 = fx_2$ and so $x_1 = x_2$.
- 3 (Orthogonal) Suppose $(A_f[x, y], A_\ell[x, y]) = (A_f[x_1, y_1], A_\ell[x_1, y_1])$ for some $f \neq \ell$. Then

$$\begin{aligned}fx + y &= fx_1 + y_1 \\ \ell x + y &= \ell x_1 + y_1\end{aligned}$$

□

Subtracting we see that $(f - \ell)x = (f - \ell)x_1$. Thus $x = x_1$ and then $y = y_1$.

EXAMPLE: $n = 5$, $\mathbb{F}_5 = \mathbb{Z}_5$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$$A_1[x, y] = x + y$$

	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

$$A_2[x, y] = 2x + y$$

	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

$$A_3[x, y] = 3x + y$$

	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$$A_4[x, y] = 4x + y$$

EXAMPLE: $n = 5$, $\mathbb{F}_5 = \mathbb{Z}_5$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$$A_1[x, y] = x + y$$

	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

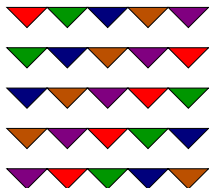
$$A_2[x, y] = 2x + y$$

	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

$$A_3[x, y] = 3x + y$$

	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$$A_4[x, y] = 4x + y$$



EXAMPLE: $n = 5$, $\mathbb{F}_5 = \mathbb{Z}_5$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$A_1[x, y] = x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

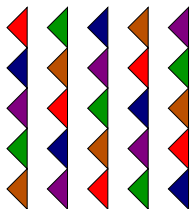
$A_2[x, y] = 2x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

$A_3[x, y] = 3x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$A_4[x, y] = 4x + y$



EXAMPLE: $n = 5$, $\mathbb{F}_5 = \mathbb{Z}_5$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$A_1[x, y] = x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

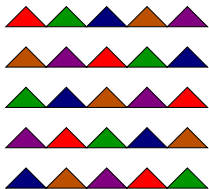
$A_2[x, y] = 2x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

$A_3[x, y] = 3x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$A_4[x, y] = 4x + y$



EXAMPLE: $n = 5$, $\mathbb{F}_5 = \mathbb{Z}_5$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$A_1[x, y] = x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

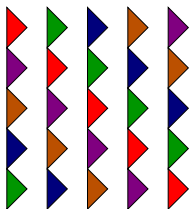
$A_2[x, y] = 2x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

$A_3[x, y] = 3x + y$

	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$A_4[x, y] = 4x + y$



EXAMPLE: $n = 5$, $\mathbb{F}_5 = \mathbb{Z}_5$.

	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$$A_1[x, y] = x + y$$



	0	1	2	3	4
0	0	1	2	3	4
1	2	3	4	0	1
2	4	0	1	2	3
3	1	2	3	4	0
4	3	4	0	1	2

$$A_2[x, y] = 2x + y$$



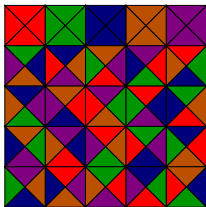
	0	1	2	3	4
0	0	1	2	3	4
1	3	4	0	1	2
2	1	2	3	4	0
3	4	0	1	2	3
4	2	3	4	0	1

$$A_3[x, y] = 3x + y$$



	0	1	2	3	4
0	0	1	2	3	4
1	4	0	1	2	3
2	3	4	0	1	2
3	2	3	4	0	1
4	1	2	3	4	0

$$A_4[x, y] = 4x + y$$



A Latin square L is *idempotent* if $L[i, i] = i$ for all i .

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

.....
IMOLS = idempotent mutually orthogonal Latin squares.

Example: 3 IMOLS(5).

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

simultaneously permute rows.

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

simultaneously permute rows.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

individually permute symbols.

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	1	2	3	4
1	2	3	4	0
2	3	4	0	1
3	4	0	1	2
4	0	1	2	3

0	1	2	3	4
3	4	0	1	2
1	2	3	4	0
4	0	1	2	3
2	3	4	0	1

0	1	2	3	4
2	3	4	0	1
4	0	1	2	3
1	2	3	4	0
3	4	0	1	2

individually permute symbols.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4

LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4

LEMMA. $k \text{ MOLS}(n) \Rightarrow k - 1 \text{ IMOLS}(n) \Rightarrow \text{OA}(k + 1, n)$ WITH n CONSTANT COLUMNS.

0	1	2	3	4
4	0	1	2	3
3	4	0	1	2
2	3	4	0	1
1	2	3	4	0

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4

3 MOLS(5)

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4


LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

3 MOLS(5)

0	3	1	4	2
3	1	4	2	0
1	4	2	0	3
4	2	0	3	1
2	0	3	1	4

0	4	3	2	1
2	1	0	4	3
4	3	2	1	0
1	0	4	3	2
3	2	1	0	4

0	2	4	1	3
4	1	3	0	2
3	0	2	4	1
2	4	1	3	0
1	3	0	2	4



LEMMA. k MOLS(n) $\Rightarrow k - 1$ IMOLS(n) \Rightarrow OA($k + 1, n$) WITH n CONSTANT COLUMNS.

3 MOLS(5)

$\begin{matrix} 0 & 3 & 1 & 4 & 2 \\ 3 & 1 & 4 & 2 & 0 \\ 1 & 4 & 2 & 0 & 3 \\ 4 & 2 & 0 & 3 & 1 \\ 2 & 0 & 3 & 1 & 4 \end{matrix}$	$\begin{matrix} 0 & 4 & 3 & 2 & 1 \\ 2 & 1 & 0 & 4 & 3 \\ 4 & 3 & 2 & 1 & 0 \\ 1 & 0 & 4 & 3 & 2 \\ 3 & 2 & 1 & 0 & 4 \end{matrix}$	$\begin{matrix} 0 & 2 & 4 & 1 & 3 \\ 4 & 1 & 3 & 0 & 2 \\ 3 & 0 & 2 & 4 & 1 \\ 2 & 4 & 1 & 3 & 0 \\ 1 & 3 & 0 & 2 & 4 \end{matrix}$
---	---	---



OA(5, 5) with 5 constant columns

0	1	2	3	4	0	0	0	0	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
0	1	2	3	4	1	2	3	4	0	2	3	4	0	1	3	4	0	1	2	4	0	1	2	3
0	1	2	3	4	3	1	4	2	3	4	2	0	1	4	0	3	4	2	0	1	2	0	3	1
0	1	2	3	4	4	3	2	1	2	0	4	3	4	3	1	0	1	0	4	2	3	2	1	0
0	1	2	3	4	2	4	1	3	4	3	0	2	3	0	4	1	2	4	1	0	1	3	0	2

C_B

OA(5, B) \setminus C_B, where B = {0, 1, 2, 3, 4}

DIRECT PRODUCT CONSTRUCTION

THEOREM

Let A be a Latin square on X and let B be a Latin square on Y . Define the square $A \times B$ on $X \times Y$ by

$$A \times B[(x_1, y_1), (x_2, y_2)] = (A[x_1, x_2], B[y_1, y_2]).$$

Then $A \times B$ is a Latin square.

Example:

X	O
O	X

 \times

1	2	3
3	1	2
2	3	1

 $=$

X1	X2	X3	O1	O2	O3
X3	X1	X2	O3	O1	O2
X2	X3	X1	O2	O3	O1
O1	O2	O3	X1	X2	X3
O3	O1	O2	X3	X1	X2
O2	O3	O1	X2	X3	X1

THEOREM

If A_1, A_2 are MOLS(m) and B_1, B_2 are MOLS(n), then $A_1 \times B_1$ and $A_2 \times B_2$ are MOLS(mn),

MACNEISE

THEOREM

If $n = p_1^{r_1} p_2^{r_2} \cdots p_x^{r_x}$, where p_1, p_2, \dots, p_x are distinct primes, then there are at least

$$M(n) = \min\{p_1^{r_1}, p_2^{r_2}, \dots, p_x^{r_x}\} - 1$$

MOLS(n).

PROOF.

- Finite field construction $\Rightarrow p_i^{r_i} - 1$ MOLS($p_i^{r_i}$) for each i .
- So there exists $M(n)$ MOLS($p_i^{r_i}$), for each i .
- Apply the direct product construction to get $M(n)$ MOLS(n).

□

Recall: MacLeish conjectures that there are at most $M(n)$ MOLS(n).

A *pairwise balanced design* PBD of type $2-(v, \mathcal{K}, \lambda)$ is a pair (X, \mathcal{B}) where

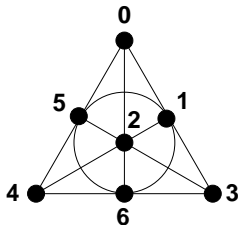
- 1 X is a v -element set of *points*,
- 2 \mathcal{B} is a collection of subsets of X called *blocks*,
- 3 $|B| \in \mathcal{K}$ for every block $B \in \mathcal{B}$, and
- 4 every pair of points is in λ blocks.

Example 1:

A PBD of type $2-(7,3,1)$ is given by:

$$X = \{0, 1, 2, 3, 4, 5, 6\}$$

$$\mathcal{B} = \{130, 124, 235, 346, 450, 156, 260\}$$



EXAMPLE: A 2-(21,5,1) PBD.

Recall: 3 MOLS(4)

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

Gave a OA(5,4)

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

Take as points

$$X = \{\infty, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3, 0, 1, 2, 3\}$$

and blocks the columns of

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

THEOREM

$n - 1$ MOLS(n) \Leftrightarrow OA($n + 1, n$) \Leftrightarrow PBD of type 2-($n^2 + n + 1, n + 1, 1$).

PBD CONSTRUCTIONS FOR MOLs

THEOREM

Let (X, \mathcal{B}) be a PBD of type $2-(v, \mathcal{K}, 1)$. Suppose for each $B \in \mathcal{B}$, there exists an k IMOLS($|B|$). Then there exists k IMOLS($|X|$).

PROOF.

- Let $\mathcal{B} = \{B_1, B_2, \dots, B_b\}$ be a $2-(v, \mathcal{K}, 1)$.
- k IMOLS(B_i) \Leftrightarrow OA($k+2, B_i$) = $C_{B_i} \cup \text{OA}(k+2, B_i) \setminus C_{B_i}$, C_{B_i} the set of constant columns.

Then $[C_X, \text{OA}(k+2, B_1) \setminus C_{B_1}, \text{OA}(k+2, B_2) \setminus C_{B_2}, \dots, \text{OA}(k+2, B_b) \setminus C_{B_b}]$

is an OA($k+2, X$) with $|X|$ constant columns, i.e. k MOLs($|X|$). □

Example: Three MOLs of order 21.

- $4 = 2^2$, is a prime power \Rightarrow 3 MOLs(4) \Rightarrow $2-(21, 5, 1)$ PBD.
- 5 is a prime power \Rightarrow 4 MOLs(5) \Rightarrow 3 IMOLS(5)
- Apply the PBD construction to get 3 MOLs(21).

This disproves the MacNeise conjecture which claimed that there would be at most

$$M(21) = \min\{3, 7\} - 1 = 2 \text{ of them}$$