Lecture 3

Orthogonal Latin Squares

NO. 1
DATE

Definition (Orthogonal L.S.). based on $\mathbb{Z}_n$ — Use $\mathbb{Z}_n$ throughout of this lecture.

Two Latin squares of order n, $L=[l_{i,j}]$ and $M=[m_{i,j}]$, are orthogonal if $\{(l_{i,j}, m_{i,j}) \mid 1 \le i,j \le n\} = \mathbb{Z}_n^2$, denoted by $L \perp M$.

e.g.

0	1	2
1	2	0
2	0	1

L

$\perp$

0	1	2
2	0	1
1	2	0

M

Let $\alpha(L)$ denote the Latin square which is obtained from L by permuting the entries of L with α (permutation of $\mathbb{Z}_n$).

Then, we have

Proposition 1 If $L \perp M$, then $\alpha(L) \perp \beta(M)$ for any two permutations α and β of $\mathbb{Z}_n$.

e.g. Let $\alpha = \begin{pmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \end{pmatrix}$, $\beta = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 2 & 1 \end{pmatrix}$.

Then, we have

1	2	0
2	0	1
0	1	2

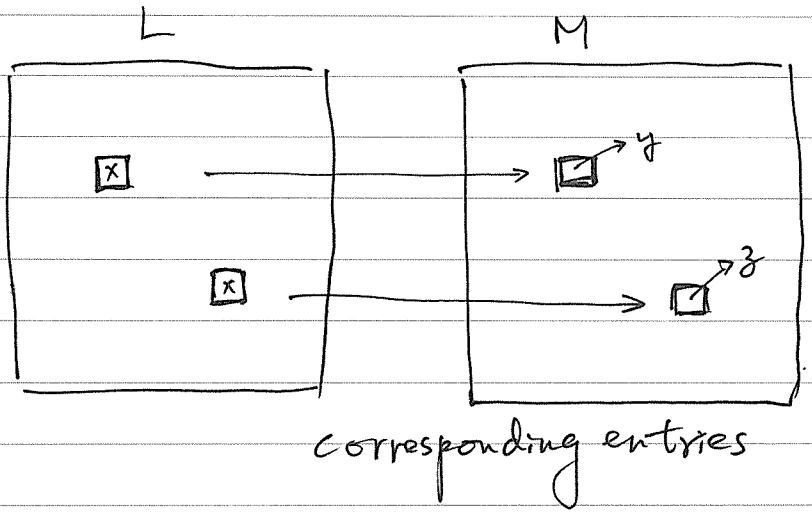
$\alpha(L)$

$\perp$

0	2	1
1	0	2
2	1	0

$\beta(M)$.

Two Finger's Rule



corresponding entries

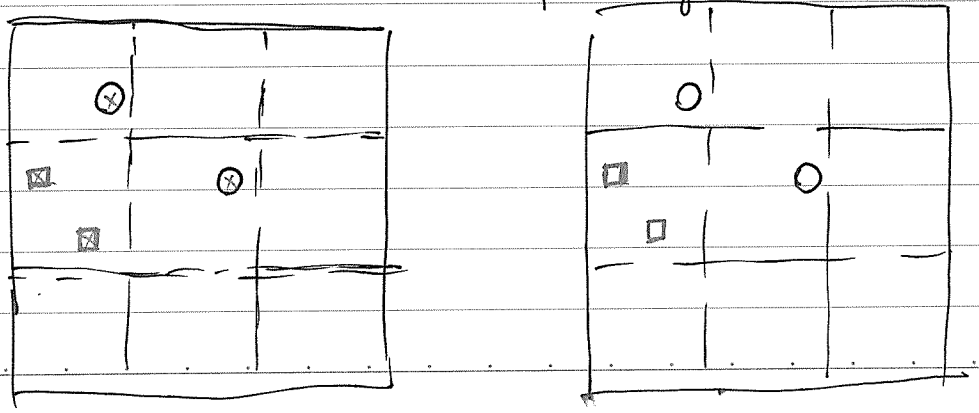
$L \perp M \iff y \neq z$ in M whenever their corresponding entries are the same entry.

$$\ell_{i,j} = \ell_{i',j'} \Rightarrow m_{i,j} \neq m_{i',j'}.$$

Proposition 2 If $L_1 \perp L_2$ (of order m) and $M_1 \perp M_2$ (of order n), then $L_1 \otimes M_1 \perp L_2 \otimes M_2$ (of order mn). ($L_1 \perp L_2, M_1 \perp M_2, N_1 \perp N_2 \Rightarrow (L_1 \otimes M_1) \otimes N_1 \perp (L_2 \otimes M_2) \otimes N_2$ and more.)

✓ **Exercise 1.4.** (10 points) Prove Proposition 2.

Consider the following two cases and use two finger's rule.



Proposition 3 If n is a prime power, then there exists $n-1$ Latin squares of order n which are mutually orthogonal.

Note. $L_1, L_2, \cdots, L_k$ are mutually orthogonal if for any two $1 \le i \ne j \le k$, $L_i \perp L_j$.

Proof. Since n is a prime power, we have a finite field $GF(n)$, $\langle F, +, \cdot \rangle$. Let $F^* = F \setminus \{0\}$. For convenience, let $F = \{0 = \alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$.

Now, we define $L^{(h)}_{i,j} = \alpha_i + \alpha_h \cdot \alpha_j$ where $\alpha_h \in F^*$. (for $0 \le i, j \le n-1$) Now, since $i \ne i'$ implies that $L^{(h)}_{i,j} \ne L^{(h)}_{i',j}$ and $j \ne j'$ implies that $L^{(h)}_{i,j} \ne L^{(h)}_{i,j'}$, $L^{(h)}$ is a Latin square. As to the orthogonality of two Latin squares, we can also use two finger's rule.

Assume that (for $(i,j) \ne (i',j')$), $L^{(h)}_{i,j} = L^{(h)}_{i',j'}$. Consider $1 \le k \ne h \le n-1$.

Suppose that $L^{(k)}_{i,j} = L^{(k)}_{i',j'}$. Then, we have

$$\begin{cases} \alpha_i + \alpha_h \cdot \alpha_j = \alpha_{i'} + \alpha_h \cdot \alpha_{j'} \\ \alpha_i + \alpha_k \cdot \alpha_j = \alpha_{i'} + \alpha_k \cdot \alpha_{j'} \end{cases}$$

$$\Rightarrow (\alpha_h - \alpha_k)\alpha_j = (\alpha_h - \alpha_k)\alpha_{j'} \Rightarrow \alpha_j = \alpha_{j'} \Rightarrow \alpha_i = \alpha_{i'}. \rightarrow\leftarrow$$

Hence $L^{(h)} \perp L^{(k)}$. ∎

Definition (A complete family of MOLS(n))

For order n, $n-1$ mutually orthogonal Latin squares form a complete family of MOLS(n).

Fact 15. If n is a prime power, then we have a complete family of MOLS(n).

Note. So far, only for prime power n, we can find a complete family of MOLS(n).

Note. It is known that there does not exist a complete family of MOLS(n) for $n = 6$ and 10.

Observation (Three MOLS(4)!)

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

$\perp$

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

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

Can we find the 3rd one by using the above two MOLS(4)?

Solve the 16 cards problem!

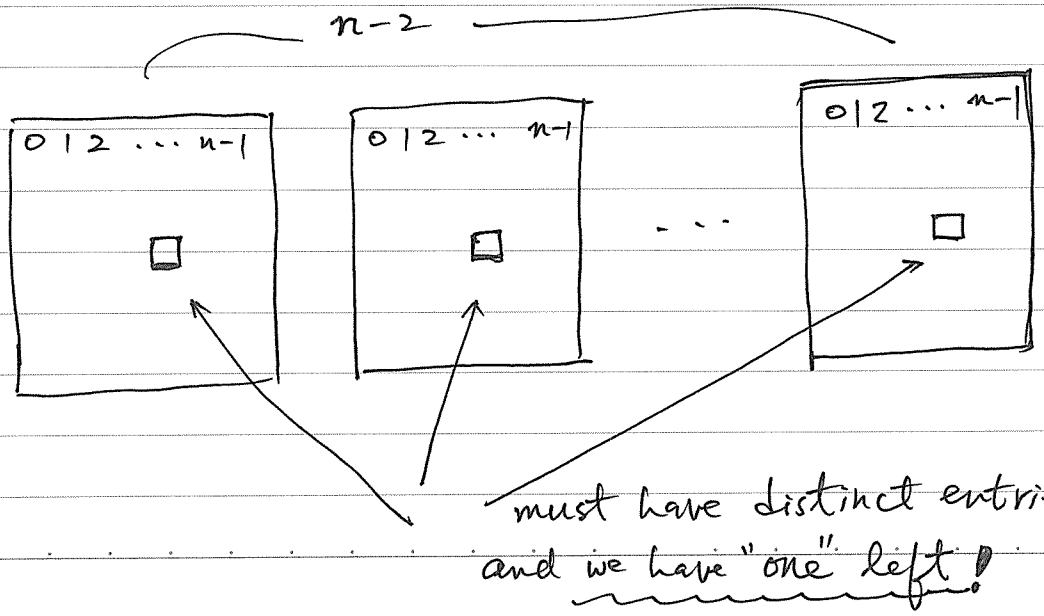
Fact 16. For each n, there are at most $n-1$ mutually orthogonal Latin squares.

Proof. By Proposition 1, we can assume all mutually orthogonal Latin squares do have the same row $(0,1,2,\cdots,n-1)$. Then, consider the $(2,1)$ cell; no two of the squares have the same entry. (?) Hence, we have at most $n-1$ distinct Latin squares which are mutually orthogonal. ∎

Proposition 4. If there exist $n-2$ MOLS(n), then we can find $n-1$ MOLS(n).

✓ Exercise 1.5. Prove Proposition 4. (10 points)

Idea:



Why "Euler" made the following conjecture?

Euler's Conjecture on MOLS.

For each $n \equiv 2 \pmod 4$, there do not exist two mutually orthogonal Latin square of order n.

(If $n > 1$ and $n \not\equiv 2 \pmod 4$, then either n is a prime or n has a prime factor larger than 2.)

Fact 17. It is true for $n = 2$ and 6 (only!). ($n = 1$ is trivial.)

Fact 18. If $n \not\equiv 2 \pmod 4$, then we can find at least two MOLS(n).

Proof. Case 1. $n \equiv 0 \pmod 4$

In this case, $n = 2^t \cdot m$ where $t \geq 2$ and m is an odd integer. If $m = 1$, then n is a prime power, the proof follows. On the other hand, if $m > 1$, then $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where p_i's are odd primes. Now, by using Proposition 2, we can construct two MOLS(n) by using direct product of two mutually orthogonal Latin squares of order $2^t, p_1^{e_1}, p_2^{e_2}, \ldots, p_k^{e_k}$ respectively.

Case 2. $n \equiv 1$ or $3 \pmod 4$

This case has been included in Case 1. ∎

Bonus (20 points) Prove that there do not exist two mutually orthogonal Latin squares of order 6.

Euler's Conjecture was disproved by Parker, Bose and Shrikhande in the year 1959. The following two MOLS(10) was proposed by E.T. Parker.

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

For $n \equiv 2 \pmod 4$ and $n \geq 10$, we need to apply ideas from pairwise balanced design to prove that two MOLS(n) do exist. (So, we will provide a proof later.)

In application, we can use another term to describe orthogonal Latin squares.

Definition (Orthogonal Array)

An orthogonal array of order n with depth k, is a $k \times n^2$ array $A = [a_{i,j}]$ such that for any two rows, the ordered pairs obtained from these two rows are exactly all ordered pairs of Z_n^2. ($a_{i,j} \in Z_n$)

OA(k, n)

e.g. OA(4,3)

$$\begin{bmatrix} 0&0&0&1&1&1&2&2&2 \\ 0&1&2&0&1&2&0&1&2 \\ 0&1&2&2&0&1&1&2&0 \\ 0&2&1&2&1&0&1&0&2 \end{bmatrix}$$

$$\Downarrow\Downarrow$$

0	0	0
1	1	1
2	2	2

0	1	2
0	1	2
0	1	2

0	1	2
2	0	1
1	2	0

0	2	1
2	1	0
1	0	2

Fact 19 the existence of an OA(k, n) is equivalent to the existence of $k-2$ MOLS(n).

Fact 20. An $OA(k,n)$ has at most n^2 columns and $n+1$ rows.

Proof. The first fact comes from the number of ordered pairs is at most n^2 and the second fact is a consequence of there are at most $n-1$ $MOLS(n)$.

In application, regularly a part of orthogonal array is sufficient. Therefore, we can use the so-called partial orthogonal array of order m with depth k. In such an array, (defined on $\mathbb{Z}_n$)
the ordered pairs are required to be distinct, not necessarily all pairs in
be $\mathbb{Z}_n^2$. Here, $m \le n^2$ (as the case in an $OA(k,n)$, but k may be larger than $n+1$.

e.g. $n=3$. $m=3$, $k=5$

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 2 & 0 \end{bmatrix}$$

Three
$\approx$ Orthogonal partial Latin squares

(*) If $m = n^2$, then $k \le n+1$.

(**) If we use each column as a codeword, then $d(C) \ge k-1$.