# Lecture 4 3,7~9

## Critical Sets and partial Transversal

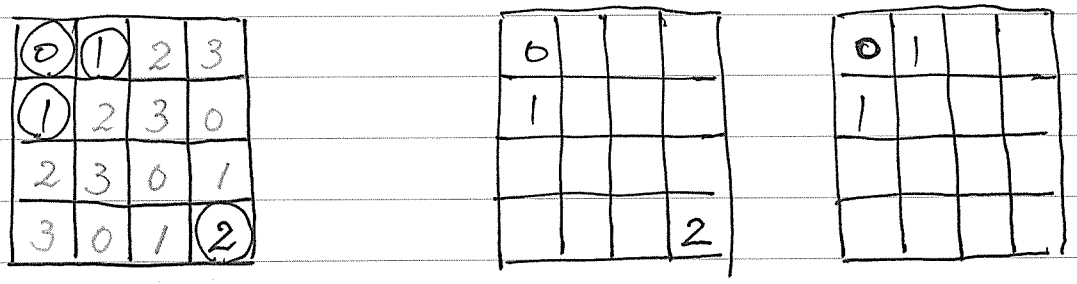
**Definition** (Critical set of L.S.)

A partial Latin square of order $n$ (PLS($n$)), $C$, is called a critical set of a Latin square $L$, if

(1) $C$ can be completed uniquely to $L$, and

(2) Any proper subset of $C$ can not be completed to a unique Latin square.

Here is an example.



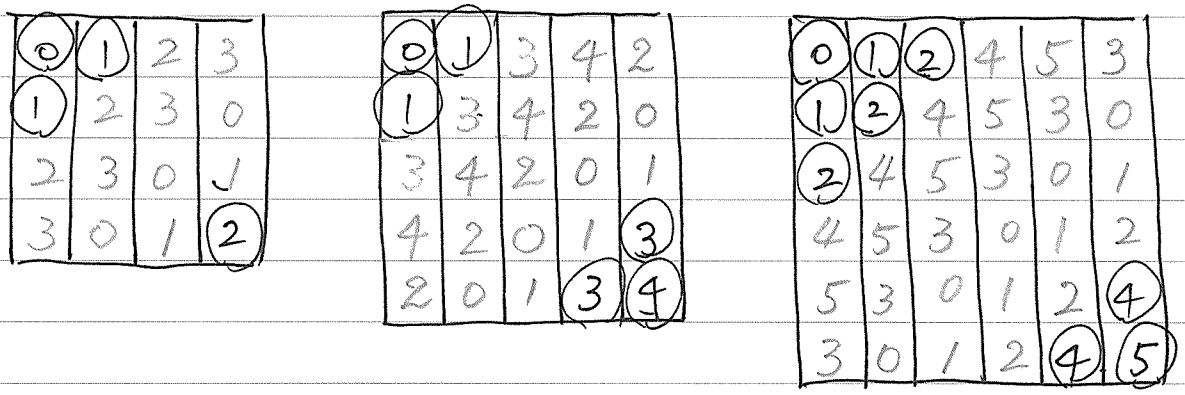

A critical set PLS(4) can not be completed uniquely

**Fact 21.** Let $C$ be a critical set of a Latin square of order $n$. Then, $C$ has at most one empty row, one empty column or one missing elements in $\mathbb{Z}_n$.

**Proof.** If one of the three cases is true, then $C$ can not be completed uniquely.

**Proposition 1** There exists a critical set $C$ of a Latin square of order $n$ with $|C| \sim \frac{n^2}{4}$.

**Proof.**




We may use the above pattern to find a critical set of size $c = (1+2+\cdots+\lfloor \frac{n}{2} \rfloor) + (1+2+\cdots+\lfloor \frac{n-1}{2} \rfloor)$. Now, if $n$ is even,

$$c = 1+2+\cdots+\frac{n}{2}+1+2+\cdots+\frac{n-2}{2} = 2(1+2+\cdots+\frac{n-2}{2})+\frac{n}{2}$$

$$= 2\cdot\frac{1}{2}\cdot\frac{n-2}{2}\cdot\frac{n}{2}+\frac{n}{2} = \frac{n^2-2n}{4}+\frac{n}{2} = \frac{n^2}{4}.$$ On the other hand, $c = \frac{n^2-1}{4}$ when $n$ is odd. ∎

So far, no critical set of size less than $\lfloor \frac{n^2}{4} \rfloor$ has been constructed. Therefore, the following conjecture remains unsettled.

**Conjecture (Critical Set)** The size of a critical set of a $LS(n)$ is at least $\lfloor \frac{n^2}{4} \rfloor$.

But, we can not apply this idea to Sudoku. It has been proved that there exists critical sets of size less than $\lceil \frac{81}{4} \rceil$, in fact, far less than that. A recent result shows that a critical set for Sudoku square is at least of size (17). The reason is very simple, since Sudoku squares do have extra properties, there are nine prescribed subsquares.

Definition (Spectrum of critical sets)

$$Spec_C(n) = \{|C| \mid C \text{ is a critical set of a L.S. of order } n\}.$$

e.g. $Spec_C(2) = 1$, $Spec_C(3) \supseteq \{2, 3\}$.

✓Exercise 1.6. Find $Spec_C(4)$. (10 points)

(*) Critical sets can be applied in constructing Sharing Scheme which is an important topic cryptography. (Key: C, partition C into several parts.)

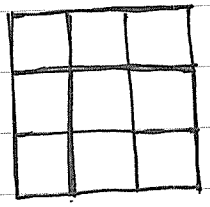
(**) The key is a Latin square of order about "50"?

Latin Square

plaintex ⟷ Ciphertex. How?

(key)

1. How to use Latin squares as keys?



Exercise 1.6'. (10 points) Use your imagination!

Exercise 1.6''. (10 points)

How to use critical sets for sharing schemes?

Definition (Sharing schemes)

$\mathcal{P}$ : participants

$\forall\ a \in \mathcal{P}$, $s(a)$ : share of $a$.

$\mathcal{K}$ (keys) : Latin squares of order $n$.

$A \subseteq \mathcal{P}$, Access structure.

Comb.$(A)$ = { combination of shares of $a \in A$ }

↓ reveals the key.

# Lecture 4 - Continued

NO. 4

DATE

## Transversal and Partial Transversal

**Definition** (Transversal)

A transversal of a Latin square of order $n$ is a set of $n$ entries, one from each row and each column, such that all the entries are distinct.

| | | | |
|---|---|---|---|
| 0 | **2** | 3 | 1 |
| **3** | 1 | 0 | 2 |
| 1 | 3 | 2 | **0** |
| 2 | 0 | **1** | 3 |

**Definition** (Partial Transversal)

A partial transversal of a Latin square (of order $n$) is a set of $m \leq n$ entries, no two of them are in the same row or the same column.

| | | | | | |
|---|---|---|---|---|---|
| **0** | 1 | 2 | 3 | 4 | 5 |
| 1 | **2** | 0 | 4 | 5 | 3 |
| 2 | 0 | 1 | **5** | 3 | 4 |
| 3 | 4 | 5 | 0 | **1** | 2 |
| 4 | 5 | **3** | 1 | 2 | 0 |
| 5 | 3 | 4 | 2 | 0 | **1** |

Fact 22. If $L \perp M$, then both $L$ and $M$ contain transversals. In fact, if $L$ (resp. $M$) is an L.S. of order $n$, then $L$ (resp. $M$) contains $n$ disjoint transversals.

Fact 23. If $L$ is a Latin square of order $n$ where $n$ is odd, then $\begin{array}{|c|c|}\hline 0&1\\\hline 1&0\\\hline\end{array} \otimes L$ contains no transversals.

Exercise 1.7. Prove Fact 23. (10 points)

- Determining whether a Latin square contains a transversal or not is a very difficult problem.
- This problem is equivalent to finding a rainbow perfect matching in an $n$-edge-colored $K_{n,n}$.

Exercise 1.8. Give examples $L'$ that $\begin{array}{|c|c|}\hline 0&1\\\hline 1&0\\\hline\end{array} \otimes L'$ contains a transversal when $L'$ is a Latin square of even order. (10 points.) $\hat{n} = 2m,\ m \in \mathbb{N}$

Ryser's Conjecture

For each Latin square of odd order, $L$, there exists a transversal.

## Revised version of Ryser's Conjecture

For each Latin square of order $n$, there exists a partial transversal which contains at least $n-1$ distinct entries (partial Transversal of size $\geq n-1$).

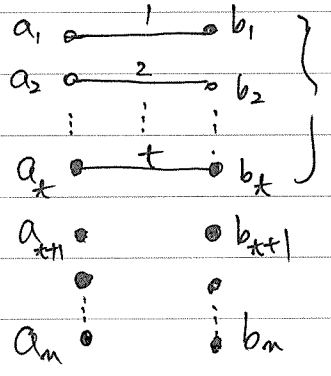
**Theorem** (P. Shor)

Let $T_n$ be a partial transversal of maximum size in a Latin square of order $n$. Then $|T_n| \geq n - O((\ln n)^2)$ or $n - c\cdot(\ln n)^2$ where $c$ is positive constant.

**Theorem** (D. Woolbright and A. E. Brouwer)

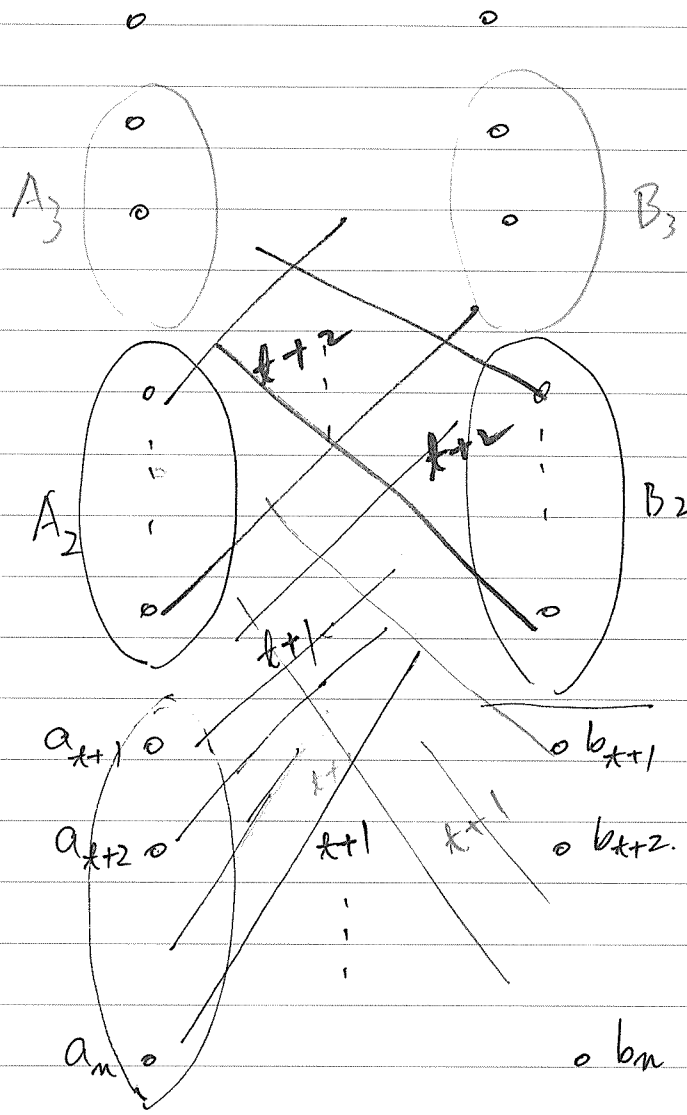
$|T_n| \geq n - \sqrt{n}$. (Bonus: 10 points for details.)

**Proof.** (Scratch) Convert an LS(n) into an $n$-edge-colored $K_{n,n}$.




Assume that $|T_n| = t$ and they are arranged as "left".

Consider the color $\underline{t+1}, \cdots, \underline{n}$ in turn.




Sometimes later

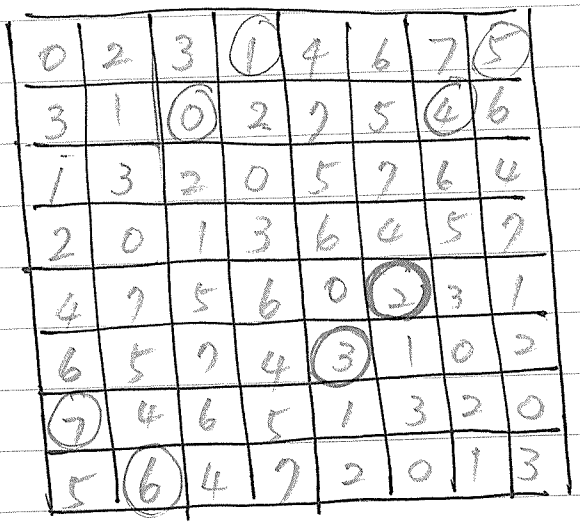
$(n-t)^2 \le n$

$\Rightarrow n-t \le \sqrt{n}$

$\Rightarrow t \ge n-\sqrt{n}$.

- $t \ge \frac{3n}{4} \Rightarrow 4t \ge 3n \Rightarrow t \ge 3(n-t)$
- Let $A_1 = \{a_{t+1}, a_{t+2}, \cdots, a_n\}$ and $B_1 = \{b_{t+1}, b_{t+2}, \cdots, b_n\}$.
- The color $t+1$ incident to $a_i$'s in $A_1$ can not be incident to $b_i$'s in $B_1$, so does the other way around.

(Bonus, 30 points) Give a talk about P. Shor's work on partial transversal.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 0 | 2 | 3 | (1) | 4 | 6 | 7 | (5) |
| 3 | 1 | (0) | 2 | 7 | 5 | (4) | 6 |
| 1 | 3 | 2 | 0 | 5 | 7 | 6 | 4 |
| 2 | 0 | 1 | 3 | 6 | 4 | 5 | 7 |
| 4 | 7 | 5 | 6 | 0 | (2) | 3 | 1 |
| 6 | 5 | 7 | 4 | (3) | 1 | 0 | 2 |
| (7) | 4 | 6 | 5 | 1 | 3 | 2 | 0 |
| 5 | (6) | 4 | 7 | 2 | 0 | 1 | 3 |

For example in finding transversal in an LS(4t).

Open problem

1. Find an algorithm to determine the maximum size of a partial transversal.

2. Given an LS(n) L, determine whether L has an orthogonal mate, i.e., find an M such that L ⊥ M if L does have an orthogonal mate, otherwise, output "No"!