Introduction to Combinatorics Lecture 9

Latin Square

The notion (concept) of 'Latin Square' probably originated with problems concerning the movement and disposition of pieces on a chess board. Its applications on agricultural design (a special type of experimental design) came out during mid-20 century. So, it is assumed to be a fairly new subject comparing to the other fields of combinational topics.

In fact, the earliest reference to the use of such squares can be dated back to 10 century. An that time, people are placing the sixteen court cards (A, K, Q, J) of a pack of ordinary playing cards in the form of a square so that no row, column, or diagonal should contain more than one card of each suit and one card of each rank. The solution was obtained in 1723. Here is an example.

A_1		K_2		Q_3		J_4	
A	1	K	2	Q	3	J	4
Q	4	J	3	A	2	K	1
J	2	Q	1	K	4	A	3
K	3	A	4	J	1	Q	2

Figure 9.1

But, the real impact comes from the famous **36 officers problem** proposed by Euler around 10 years later. So, 16 cards are extended to 36 cards. Unfortunately, this plan turns out to be impossible. The proof by 'brute force' was obtained around 1900 by Tarry. A theoretical argument to show that it is not possible came out after around 80 years by D. R. Stinson (1984).

Nowadays, the applications of using Latin Squares have been everywhere.

Definition 9.1 (Latin Square of order n)**.** A Latin square of order n, L, is an $n \times n$ array based on a n-set S ($\mathbb{Z}_n$ for convenience) such that each element of S occurs in each row and each column exactly once.

Example. Latin square of order 3. Note that we can use any n-set for S, say $S = \{\alpha, \beta, \gamma\}$.

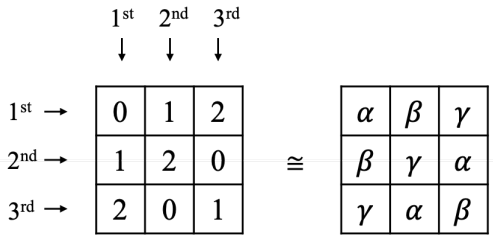


Figure 9.2: Latin square of order 3.

We use $L_{i,j}$ to denote that (i, j)-entry in L where i (resp. j) is the row (resp. column) number . If L is of order n, then the row (column) numbers are $1, 2, ..., n$. (Even we use $0, 1, 2, ..., n-1$ for the number of side line or head line.)

Facts.

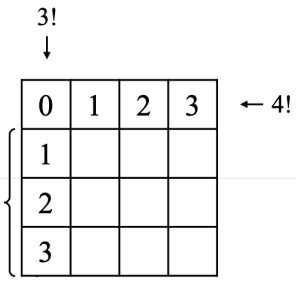
1. A Latin square of order n exists for each $n \in \mathbb{N}$.
2. A Latin square of order n can be obtained from the fact $\chi'(K_{n,n}) = n$ (edge coloring of $K_{n,n}$).
3. The existence of a Latin square of order n is equivalent to the existence of $K_3 \mid K_{n,n,n}$ (graph decomposition).
4. Let ℓ_n denoted the number of distinct Latin sequences of order n. Then, $\ell_1 = 1,\ \ell_2 = 2,\ \ell_3 = 12,\ \ell_4 = 576,\ \ell_5 = 161280,\ ....$ ($L \neq L'$ if and only if $L_{i,j} \neq L'_{i,j}$ for some (i, j).)
5. $\ell_9 = 9!8!\ (377, 597, 964, 258, 816)$. Check Wiki for more information!

A Latin square of order n can be obtained from the operation table of a 'quasigroup' of order n. For example, $S = \{0, 1, 2\}$, $\langle S, * \rangle$ is a quasigroup of order 3.

$*$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Figure 9.3: Quasigroup of order 3.

By using permutations of $0, 1, 2, 3$, we can obtain a Latin square of 'standard form':



Now, there are 4 ways to finish filling all the other entries by choosing 'typical' entries first (circled entry in Figure 9.4). (Similar to Sudoku.)

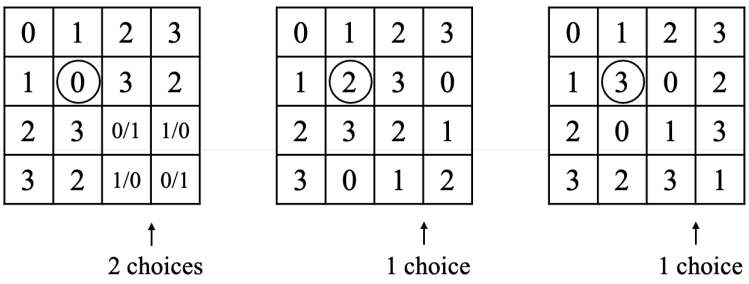


Figure 9.4: 4 non-isomorphic Latin squares of order 4.

Basically, this is the idea of counting distinct Latin squares. Hence, $\ell_4 = 4 \times 4! \times 3! = 576$, $\ell_5 = \textcircled{?} \times 5! \times 4!$, $\textcircled{?} = 56$. (?)

Algebraic Structure

Definition 9.2 (Binary operation)**.** A binary operation defined on A is a mapping $circ : A \times A \to A$. For convenience, $\circ((c, b)) = c$ is denoted by $a \circ b = c$.

Remark. For $t \geq 2$, we can define a t-ary operation defined on A as a mapping $f : A^t \to A$.

Definition 9.3 (Algebraic structure in one operation)**.** An order pair $\langle A, \circ \rangle$ is a *groupoid* if '$\circ$' is a binary operation defined on A.

Besides binary operation, an operation may satisfy more 'laws':

① Associative law: $\forall a, b, c \in A,\ a \circ (b \circ c) = (a \circ b) \circ c$.

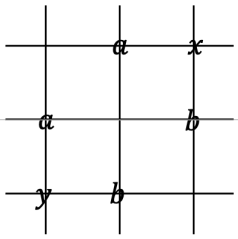
② Commutative law: $\forall a, v \in A,\ a \circ b = b \circ a$.

③ Identity: e is an identity of $\langle A, \circ \rangle$ if $\forall a \in A,\ a \circ e = e \circ a = a$.
Right identity: $a \circ e = a$.
Left identity: $e \circ a = a$.

④ Inverse: a is an inverse of b (in A) if $a \circ b = b \circ a = e$.
Right inverse: $a \circ b = e$.
Left inverse: $b \circ a = e$.

⑤ Row Latin property: $\forall a, b \in A,\ a \circ x = b$ has a unique solution in A.

⑥ Column Latin property: $\forall a, b \in A,\ y \circ a = b$ has a unique solution in A.



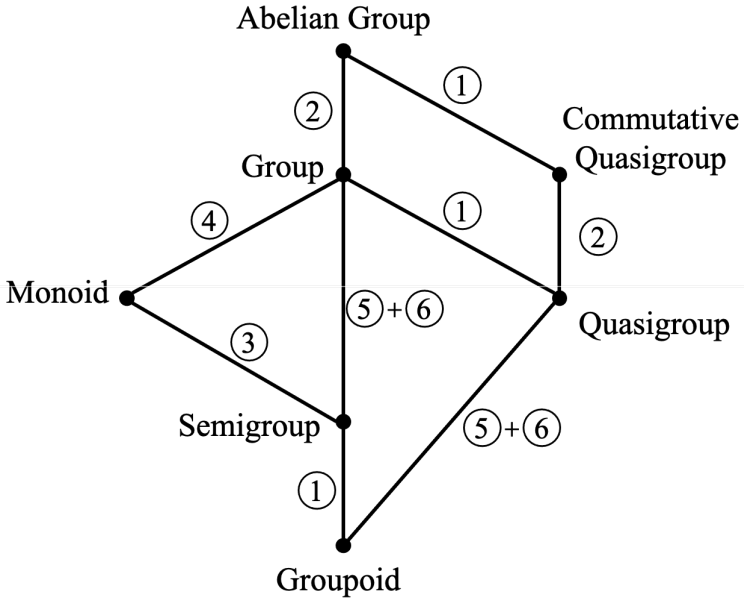
Remark.

- If ⑤ is true, then the row 'a' has distinct entries, further more, all elements in A occur! (If we have two common entries in a row, then 'x' is not unique.)
- If ⑥ is true, then the column 'a' has distinct entries of A. (Similar reason.)

Definition 9.4 (Quasigroup)**.** If $\langle A, \circ \rangle$ satisfies row and column Latin properties, then $\langle A, \circ \rangle$ is a quasigroup. If A is a finite set, then its operation table corresponds to a Latin square of order $|A|$.

Some basic structures. ($\textcircled{0}$: $\langle A, \circ \rangle$ is a groupoid.)

1. $\textcircled{0} + \textcircled{1}$ = Semigroup
2. $\textcircled{0} + \textcircled{1} + \textcircled{3}$ = Monoid
3. $\textcircled{0} + \textcircled{1} + \textcircled{3} + \textcircled{4}$ = Group
4. $\textcircled{0} + \textcircled{1} + \textcircled{2} + \textcircled{3} + \textcircled{4}$ = Abelian Group
5. $\textcircled{0} + \textcircled{5} + \textcircled{6}$ = Quasigroup
6. $\textcircled{0} + \textcircled{1} + \textcircled{5} + \textcircled{6}$ = Group
7. $\textcircled{0} + \textcircled{2} + \textcircled{5} + \textcircled{6}$ = Commutative Quasigroup



Definition 9.5 (Idempotent and Unipotent)**.** A quasigroup $\langle Q, * \rangle$ is idempotent if for each $a \in Q,\ a * a = a$. $\langle Q, * \rangle$ is unipotent if for each $a \in Q,\ a * a = c$ (a constant in Q).

Example.

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

(a)

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

(b)

Figure 9.5: (a) Idempotent and commutative L.S. $\approx \chi'(K_n) = n$ (n is odd).
(b) Unipotent and commutative L.S. $\approx \chi'(K_n) = n - 1$ (n is even).

Remark. To construct an idempotent commutative Latin square for each odd n, we define an abelian group $\langle \mathbb{Z}_n, + \rangle$. For example, $n = 7$. Then, permuting the entries.

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Figure 9.6: Operation table of $\langle \mathbb{Z}_7, + \rangle$.

Facts.

6. We shall adapt the property of a quasigroup of order n to 'claim' the property of its corresponding Latin square.
   For example, if $\langle Q, * \rangle$ is a commutative quasigroup of order n, then its corresponding Latin square is a commutative Latin square or sometimes a 'symmetric' Latin square.

7. Let $\langle Q, * \rangle$ be a quasigroup. Define $\langle Q, \circ \rangle$ where $a \circ c = b$ provided $a * b = c$ for all $a, b, c \in Q$. Then, $\langle Q, \circ \rangle$ is also a quasigroup (conjugate).
   Note that $a * b = c \ \Rightarrow a \circ c = b,\ b \circ' a = c,\ \underline{b \circ'' c = a},\ c \circ''' a = b,\ c \circ'''' b = a.$

$\forall a, b \in Q,\ a \circ'' x = b$ has unique solution $c \in Q$ since $c * b = a$. Similarly, $y \circ'' a = b$ has a solution c' if $a * b = c'$. They are called conjugate quasigoups and therefore we have conjugate Latin squares of order 3.

$\circ$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	0	1	2
0	0	1	2
1	2	0	1
2	1	2	0

$0 \circ 0 = 0$
$0 \circ 1 = 1$
$0 \circ 2 = 2$
$1 \circ 0 = 1$
$1 \circ 1 = 2$
$1 \circ 2 = 0$
$2 \circ 0 = 2$
$2 \circ 1 = 0$
$2 \circ 2 = 1$

$\uparrow\ \uparrow\ \uparrow$
a b c

$0 \circ 0 = 0$
$0 \circ 1 = 1$
$0 \circ 2 = 2$
$1 \circ 1 = 0$
$1 \circ 2 = 1$
$1 \circ 0 = 2$
$2 \circ 2 = 0$
$2 \circ 0 = 1$
$2 \circ 1 = 2$

$\uparrow\ \uparrow\ \uparrow$
a c b

Figure 9.7: Conjugate quasigroups.

Definition 9.6 (Isotopism)**.** Two quasigroups $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic if there exist three bijections $\alpha,\ \beta$ and γ from Q_1 onto Q_2 such that $\gamma(x \circ y) = \alpha(x) * \beta(y)$ for any two elements $x, y \in Q_1$. If $\alpha = \beta = \gamma$, then $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic.

Remark.

- If $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are isotopic, then we say there exists an isotopism between $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$. Check that 'isotopism' is an equavalence relation!
- Since isotopism is an equivalence relation, we can partition the set of distinct Latin squares of order n into isotopic classes. For example, there are two isotopic classes of order 4 and 22 isotopic classes of order 6. (Only one isotopic class for order 1,2 and 3; and two classes for order 4.)

Partial Latin Square

Over past 30 years, several important progress in solving open problems on Latin squares has been done by applying graph technique. The main idea comes from the following correspondence.

Let $G = (V, E)$ be a graph. A k-edge-coloring π of G is a mapping $\pi : E \to \{1, 2, ..., k\}$ such that $\pi(e) \neq \pi(f)$ provided e and f are incident edges in G. The minimum integer k such that G has a k-edge-coloring is called the chromatic index of G, denoted by $\chi'(G)$. The following facts are well-known in Graph Theory.

Facts.

8. If G is a simple graph, then $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.
9. If G is a bipartite graph, then $\chi'(G) = \Delta(G)$.
10. The edge-coloring $\chi'(K - n, n)$ corresponds to a Latin square of order n.

Remark.

- The number of distinct n-edge-colorings of $K_{n,n}$ gives ℓ_n, see Figure 9.8.

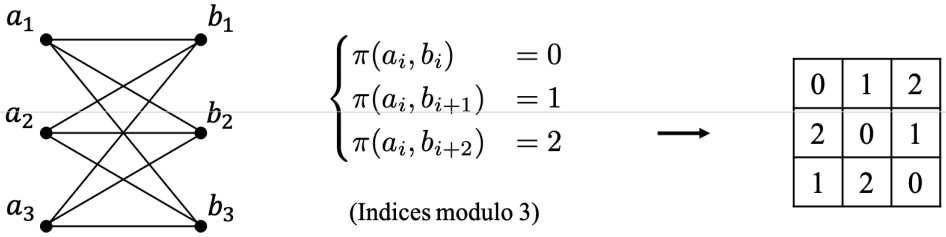
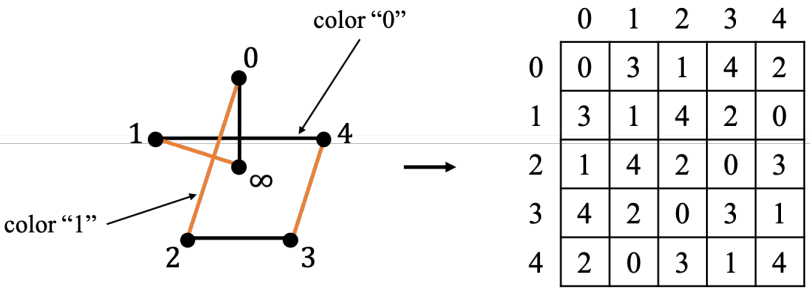


Figure 9.8: $n = 3$.

- A unipotent Latin square of order n can be constructed accordingly.
- We can use $\chi'(K_{2m+1}) = 2m + 1$ to construct an idempotent commutative Latin square, see Figure 9.9.
- There does not exist an idempotent commutative Latin square of even order.



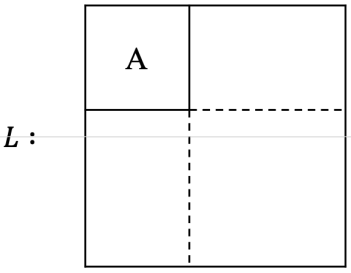
	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

Figure 9.9: $m = 2$.

Just like algebraic structures, we have sub-quasigroups and subsquares.

Definition 9.7 (Sub-Latin square)**.** If $Q' \subseteq Q$, $\langle Q', \circ \rangle$ and $\langle Q, \circ \rangle$ are quasigroups, then $\langle Q', \circ \rangle$ is called a sub-quasigroup of $\langle Q, \circ \rangle$. Their corresponding Latin squares are Latin square and Latin subsquare respectively.

Definition 9.8 (Embedding)**.** If A is a sub-Latin square (or Latin subsquare) of L, then A is said to be embedded in L. The standard form is the one with A in the upper left hand corner.



Theorem 9.1. *A Latin subsquare of order m can be embedded in a Latin square of order n if and only if $n \geq 2m$.*

Facts.

11. If L (of order n) has a Latin subsquare A (of order m), then n may not be a multiple of m. (It is true $m \mid n$ if both L and A are corresponding to a group.)

In what follows, we provide some more insight above having a subsquare.

Proposition 9.2. *If A is embedded in L and $L(i)$ denotes the number of element i occurs in L (respectively A, B, C, D in Figure 9.10), then $A(i) \geq 2m - n$ where A is a Latin square of order m and L is a Latin square of order n.*

Proof. $\forall i \in \mathbb{Z}_n$, since $B(i) + D(i) = n - m$, $B(i) \leq n - m$ and $A(i) + B(i) = m$. Hence, $A(i) = m - B(i) \geq m - (n - m) = 2m - n$. □

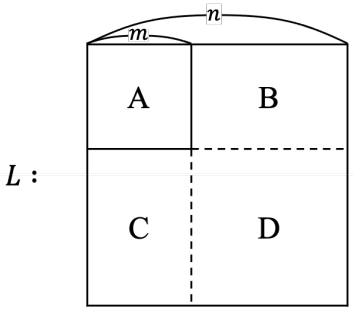


Figure 9.10

Corollary 9.3. *A Latin subsquare of order m can be embedded in a Latin square of order n, then $n \geq 2m$. (The sufficient condition of Theorem 9.1 is true.)*

Proof. If $n < 2m$, then every $i \in \mathbb{Z}_n$ has to occur in A, which is not possible since A is a Latin square of order m. □

Remark. The subsquare A we consider here can be replaced by Latin rectangle or partial Latin rectangle, denoted as R.

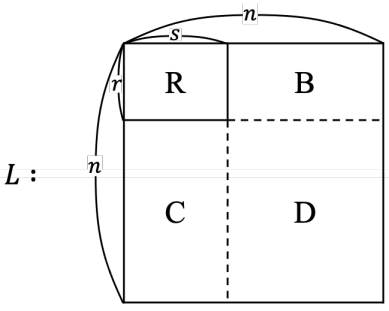


Figure 9.11

Proposition 9.4. *If R is embedded in a Latin square L which is based on S, then $\forall i \in S,\ R(i) \geq r + s - n$.*

Proof. $R(i) + B(i) = r,\ B(i) + D(i) = n - s$ and $B(i) \leq n - s$. Hence, $R(i) = r - B(i) \geq r - (n - s)$. □

Proposition 9.5. *Let R be a $r \times n$ Latin rectangle based on an n-set S. Then R can be embedded in a Latin square of order n.*

Proof. SDR (system of distinct representatives) or König's Theorem. □

0	1	2	3	4
3	2	4	1	0
A_1	A_2	A_3	A_4	A_5

$A_1 = \{1, 2, 4\}$
$A_2 = \{0, 3, 4\}$
$A_3 = \{0, 1, 3\}$
$A_4 = \{0, 2, 4\}$
$A_5 = \{1, 2, 3\}$

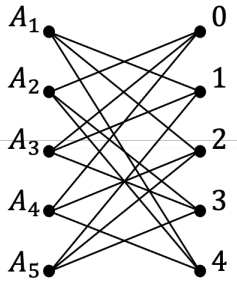


Figure 9.12

Proposition 9.6. *Let R be a $r \times n$ partial Latin rectangle. Then R can be embedded in a Latin square of order n based on S if and only if $R(i) \geq r + s - n\ \forall i \in S\ (|S| = n)$.*

Proof. (Outline)

Step 1. Fill all the entries in R such that the condition $R(i) \geq r + s - n$ holds.

Step 2. Fill in the entries in B. (Obtain a $n \times n$ Latin rectangle.)

Step 3. Complete the Latin square by extending the rectangle. The details are obtained by using two theorems related to the existence of SDR's. (?) □