Chapter 1

Latin Squares

1.1 Latin Squares

Definition 1.1.1. A *latin square* of order n is an $n \times n$ array in which n distinct symbols are arranged so that each symbol occurs exactly once in each row and column.

If the set of n distinct symbols is S, then we say the latin square is based on S. For convenience, we shall take the set of n distinct symbols be $\mathbb{Z}_n = \{0, 1, 2, \cdots, n-1\}$.

Example 1.1.2.

0

,

0	1
1	0

,

0	1	2
1	2	0
2	0	1

, • • •

By observation of the above examples, it is easy to see

($*1$) for each positive integer n, there exists a latin square of order n.

A latin square L of order n can also be denoted by $L = [l_{i,j}]_{n\times n}$ where $l_{i,j} \in \mathbb{Z}_n$. Let α, β, γ be three permutations of $\mathbb{Z}_n$. Then, we use $L_{(\alpha)}, L^{(\beta)}$, and $\gamma(L)$ to denote the latin squares obtained from L by permuting the rows with α, the columns with β and the entries $l_{i,j}$ with γ respectively. Clearly,

($*2$) $L_{(\alpha)}, L^{(\beta)}$, and $\gamma(L)$ are latin squares for all permutations α, β, and γ.

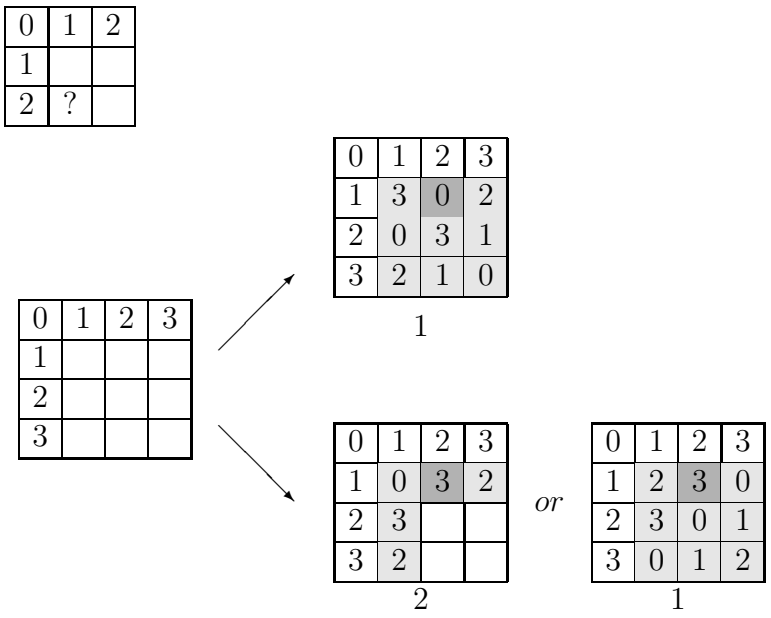
($*3$) The latin square obtained by applying the above three operations to L (simultaneously) is denoted by $L(\alpha, \beta, \gamma)$.

Definition 1.1.3. A latin square $L = [l_{i,j}]$ of order n is said to be a *standard* latin square (or reduced latin square) if $l_{i,0} = i$ and $l_{0,j} = j$ where the rows and columns are indexed by $0, 1, 2, \cdots, n-1$.

Notations Let L_n and ℓ_n denote the number of latin squares and standard latin squares respectively.

Proposition 1.1.4. $L_1 = \ell_1 = 1$, $L_2 = 2$ and $\ell_2 = 1$, $L_3 = 12$ and $\ell_3 = 1$, $L_4 = 576$ and $\ell_4 = 4$.

Proof.



∎

Proposition 1.1.5. $L_n = n!(n-1)!\ell_n$.

Proof. There are $n!$ ways to permute the entries of the first row and then there are $(n-1)!$ ways to the rest $n-1$ rows in order to obtain a standard latin square. ∎

Example 1.1.6. By using computer, we have

$$\ell_6 = 9,408 \quad \text{and} \quad \ell_{10} = 7,580,721,483,140,132,811,489,280.$$

Note $\ell_{15} \approx$(Estimate) $1.5 \cdot 10^{86}$. $L_{15} \approx 15! \cdot 14! \cdot 1.5 \cdot 10^{86}$.

Exercise 1.1.7. Find the number of distinct latin squares of order 9 which are corresponding to all the possible solutions of "Sudoku". (Difficult!)

1.2 Quasigroups

Definition 1.2.1. Let S be a nonempty set. Then a function $f : S \times S \to S$ is called a *binary operation* on S and a function $f : S^r \to S$ is an r-ary operation on S. For convenience, when binary operations are considered, we use afb to denote $f((a,b)) = f(a,b)$ where $(a,b) \in S \times S$.

Example 1.2.2. Let $S = \mathbb{Z}$(the set of integers). Then $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ is a binary operation on $\mathbb{Z}$. $+(a,b) = a+b$.

Note An algebraic structure contains a nonempty set S and several operations on S, denoted by $\langle S; \ldots \rangle$.

Definition 1.2.3. If $\circ$ is a binary operation on S, then $\langle S; \circ \rangle$ is a *groupoid*.

Definition 1.2.4. If $\langle S; \circ \rangle$ is a groupoid and $a \circ (b \circ c) = (a \circ b) \circ c$ for any three elements $a, b, c \in S$, then $\langle S; \circ \rangle$ is a *semi-group* and the operation is an associative operation on S.

Question Do you have an idea to determine whether "$\circ$" is an associative operation on S in a faster way?

Definition 1.2.5. If $\circ$ is a groupoid and both $a \circ x = b$ and $y \circ c = d$ have unique solution (for x and y) respectively for $a, b, c, d \in S$, then $\langle S; \circ \rangle$ is a *quasi-group*.

Proposition 1.2.6. Let $S = \{0, 1, 2, \cdots, n-1\}$ and $\langle S; \circ \rangle$ be a quasi-group. Then, by deleting headline and sideline of the operation-table, we obtain a latin square of order n.

Therefore, if we fix the headline and sideline of a quasi-group, we obtain a unique latin square. Similarly, we can obtain a quasi-group by using a latin square. From this observation, we can study latin square with special properties via the structure of its corresponding quasi-group.

Definition 1.2.7. Let $\langle Q; \circ \rangle$ be a quasi-group. Then

1. $\langle Q; \circ \rangle$ is *associative* if $a \circ (b \circ c) = (a \circ b) \circ c, \forall a, b, c \in Q$.
2. $\langle Q; \circ \rangle$ is *commutative* if $a \circ b = b \circ a, \forall a, b \in Q$.
3. $\langle Q; \circ \rangle$ is *semi-symmetric* if $a \circ (b \circ a) = b, \forall a, b \in Q$.
4. $\langle Q; \circ \rangle$ is *totally symmetric* if $a \circ (a \circ b) = b$ and $(a \circ b) \circ b = a, \forall a, b \in Q$.
5. $\langle Q; \circ \rangle$ is *idempotent* if $a \circ a = a, \forall a \in Q$.
6. $\langle Q; \circ \rangle$ is *unipotent* if $a \circ a = c$ where c is a fixed element in Q and a is arbitrary.

Proposition 1.2.8. If $\langle G; \circ \rangle$ is totally symmetric, then $\langle G; \circ \rangle$ is commutative.

Proof. $(a \circ (a \circ b)) \circ (a \circ b) = a \Rightarrow b \circ (a \circ b) = a$.
$b \circ a = b \circ (b \circ (a \circ b)) = (a \circ b) = a \circ b$. ∎

Proposition 1.2.9. A commutative idempotent latin square of order n exists if and only if n is an odd positive integer.

Proof. Since each element of $\{0, 1, 2, \cdots, n-1\}$ occurs exactly once in the diagonal and occurs outside of diagonal in pairs, the total occurrence of each element is odd.

Let $L = [\ell_{i,j}]_{n \times n}$ be defined on $\mathbb{Z}_n$ by letting $l_{i,j} = i + j \pmod{n}$. Since n is odd, L is a diagonal latin square and a commutative latin square. By permuting the diagonal with a suitable permutation, we obtain an idempotent commutative latin square. See the following figure for an example.

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

$\Longrightarrow$

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

∎

Proposition 1.2.10. If an idempotent totally symmetric latin square of order n exists then $n \equiv 1$ or $3 \pmod{6}$.

Proof. Let L be an idempotent totally symmetric latin square. $\forall a, b, c$ distinct elements, let $a \circ b = c$. Then $b \circ a = c, a \circ c = b, c \circ a = b, b \circ c = a, c \circ b = a$. This implies that the number of entries outside of the diagonal of L is a multiple of "6". (?) Hence $6|n^2 - n$. By proposition 1.2.9, n is odd. So, $n \equiv 1$ or $3 \pmod 6$. ∎

Question Is the above necessary condition also sufficient?
Note The study of constructing latin squares with certain properties is commonly considered as the main topic in Universal Algebra. Since a quasi-group does not require the "Associative Law", it is sometimes referred to as a topic in "Non-associative Algebra". For consistency, we shall use the term "latin square" instead of quasi-group throughout the rest of this chapter.

Definition 1.2.11. A *latin subsquare* A (of order m) of a latin square L of order n, is a sub-array of L such that $a_{i,j} = l_{i,j}$ for $1 \leq i, j \leq m$ and A itself is a latin square of order m. Here $L = [l_{i,j}]_{n \times n}$, $A = [a_{i,j}]_{m \times m}$ and $m \leq n$.

$(*4)$ $m \leq \frac{n}{2}$ provided that A is a subsquare of L.

$(*5)$ $m|n$ is not necessary. (Note that if A and L are corresponding to groups, then m has to be a divisor of n by *Lagrange's Theorem*.)

Example 1.2.12. A latin square of order 5 with a subsquare of order 2.

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

Definition 1.2.13. If A is a subsquare of L, we also call A is *embedded* in L.

Definition 1.2.14. An $m \times n$ *latin rectangle* R is an $m \times n$ array ($m \leq n$) based on $\mathbb{Z}_n$ such that each element of $\mathbb{Z}_n$ occurs in each row and column of R at most once. (For rows, occurs exactly once.)

Definition 1.2.15. Let $m < n$. An $m \times n$ latin rectangle is said to be extended to a latin square of order n if we can add $n - m$ rows to the rectangle such that the resulting square is a latin square.

Example 1.2.16.

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

Add two rows to a rectangle.

Proposition 1.2.17. Every $m \times n$ latin rectangle with $m < n$ can be extended to a latin square of order n.

Before we prove this proposition, we introduce a notion called *SDR*.

Definition 1.2.18. (System of Distinct Representative)

Let $\{A_1, A_2, \cdots, A_n\}$ be a collection of n sets. Then, we say $(a_1, a_2, \cdots, a_n)$ is a system of distinct representatives (SDR) of $\mathcal{A} = \{A_1, A_2, \cdots, A_n\}$ if $a_i \in A_i$ and $a_i \neq a_j$ for $1 \leq i < j \leq n$.

Theorem 1.2.19. (Hall's Condition)

$\{A_1, A_2, \cdots, A_n\}$ has an SDR if and only if $\left|\bigcup_{j=1}^{k} A_{i_j}\right| \geq k$ for $1 \leq k \leq n$.

Proof. ($\Rightarrow$) Easy to see.

($\Leftarrow$) By induction on the number of sets in the collection. Clearly, it is true for $n = 1$ Assume that the assertion is true for n and let $\mathcal{A} = \{A_1, A_2, \cdots, A_{n+1}\}$ be a collection of $n+1$ sets which satisfies the Hall's condition: any collections of k sets contains at least k distinct elements.

First, if any collection of k sets in $\mathcal{A} = \{A_1, A_2, \cdots, A_n\}$ consists more than k distinct elements. Let $a_{n+1} \in A_{n+1}$ and consider $\mathcal{A}' = \{A_1 - a_{n+1}, A_2 - a_{n+1}, \cdots, A_n - a_{n+1}\}$. Then, by assumption $\mathcal{A}'$ has an SDR $(a_1, a_2, \cdots, a_n)$. Hence, $(a_1, a_2, \cdots, a_n, a_{n+1})$ is an SDR of $\mathcal{A}$. On the other hand, if there exists a collection of h sets in $\{A_1, A_2, \cdots, A_n\}$, say $\{A_1, A_2, \cdots, A_h\}$ such that $\left|\bigcup_{j=1}^{h} A_i\right| = h$, let $\bigcup_{j=1}^{h} A_i = A$. Then, consider $\{A_{h+1} \setminus A, A_{h+2} \setminus A, \cdots, A_{n+1} \setminus A\}$. Since, $h \leq n$, this is not an empty collection. Moreover, let (W.L.O.G.) $A_{h+1} \setminus A, A_{h+2} \setminus A, \cdots, A_{h+k} \setminus A$ be any collection of k sets. Then, $\bigcup_{i=1}^{k} A_{h+i} \setminus A = \bigcup_{i=1}^{k} (A_{h+i} \cap A') = A' \cap \left(\bigcup_{i=1}^{k} A_{h+i}\right)$ has at least k elements. For otherwise, $\bigcup_{i=1}^{h+k} A_i$ contains less than $h+k$ elements which contradicts to the Hall's condition. Therefore, $\{A_{h+1} \setminus A, A_{h+2} \setminus A, \cdots, A_{n+1} \setminus A\}$ has an SDR $(a_{h+1}, a_{h+2}, \cdots, a_{n+1})$. Also, by induction $\{A_1, A_2, \cdots, A_h\}$ has an SDR $(a_1, a_2, \cdots, a_h)$. By combining them, we have the proof. ∎

Now, we are ready to prove Proposition 1.2.17.

Proof. Let A_i be the set of elements in $\mathbb{Z}_n$ which do not occur in the ith column of the latin rectangle $R = [r_{i,j}]_{m \times n}$. Then, by definition, any collection of k sets in $\{A_1, A_2, \cdots, A_n\}$ contains at least k elements in $\mathbb{Z}_n$.(?) Therefore, we have an SDR which can be placed as the $(m+1)^{th}$ row of the rectangle. By continuing the process, we are able to obtain a latin square of order n which contains R as a subarray. ∎

Theorem 1.2.20. *A latin square of order m can be embedded in a latin square of order n if and only if $m \leq \frac{n}{2}$.*

Proof. Exercise. ∎

Theorem 1.2.21. *Let $\langle Q; \circ \rangle$ be a quasi-group which is associative. Then $\langle Q; \circ \rangle$ is a group.*

Proof. Let $a \in Q$. Then $\exists!$ e_a, such that $a \circ e_a = a$. (Unique solution.) And, $\forall b \in Q$, $\exists!$ $y_b \circ a = b$. ($y \circ a = b$ has a unique solution.)

Now, $b \circ e_a = (y_b \circ a) \circ e_a = y_b \circ (a \circ e_a) = y_b \circ a = b$. This implies that e_a is a right identity of $\langle Q; \circ \rangle$. By a similar argument, let $e'_a \circ a = a$. Then, $\forall c \in Q$, $e'_a \circ c = e'_a \circ (a \circ x_c) = (e'_a \circ a) \circ x_c = a \circ x_c = c$. e'_a is a left identity of $\langle Q; \circ \rangle$.

Hence, $e_a = e'_a \circ e_a = e'_a$. Let $e = e_a = e'_a$. Then, e is an identity of $\langle Q; \circ \rangle$.

It's left to show that $\forall a \in Q$, a has an inverse.

Clearly, there exists an a', such that $a' \circ a = e$ and an a'' such that $a \circ a'' = e$, both of them are unique. But, now, $a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a''$. This concludes the proof. ∎

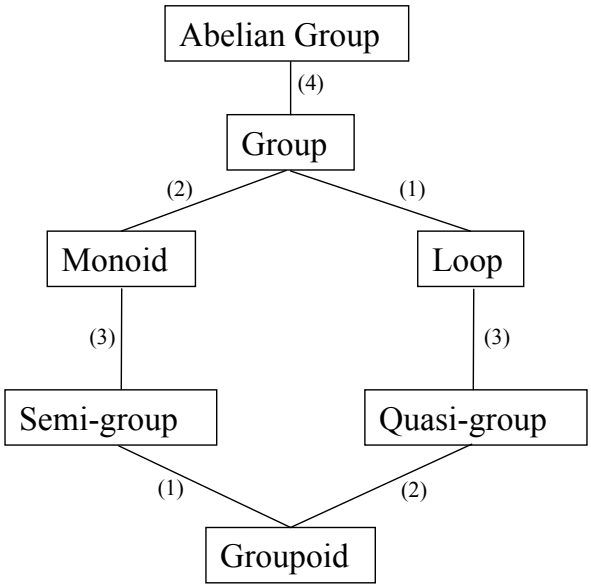


Figure 1.1: Algebraic Structures with one operations.

(1) Associative Law
(2) Latin Property
(3) Identity Element
(4) Commutative Law

1.3 Algebraic Structure with Two Operations

Definition 1.3.1. (Ring)

A *ring* $(R; +, \cdot)$ is a set R, together with two binary operations, denoted by "+" and "$\cdot$", such that

1. R is an abelian group with respect to $+$, or, $\langle R; + \rangle$ is an abelian group.
2. "$\cdot$" is associative.
3. The distributive laws hold; i.e., $\forall a, b, c \in R, a \cdot (b+c) = a \cdot b + a \cdot c$ and $(a+b) \cdot c = a \cdot c + b \cdot c$.

Definition 1.3.2. A ring $(R; +, \cdot)$ together with multiplicative identity is a *ring with identity*. A ring $(R; +, \cdot)$ is *commutative* if "$\cdot$" is commutative.

Definition 1.3.3. A commutative ring with identity $e \neq 0$ is an *integral domain* if $ab = 0$ implies $a = 0$ or $b = 0$.

Definition 1.3.4. A ring is called a *division ring* if $\langle R \setminus \{0\}; \cdot \rangle$ is a group.

Definition 1.3.5. (Field)
A commutative division ring is called a *field*.

Definition 1.3.6. $\langle F; +, \cdot \rangle$ is a field if

1. $\langle F; + \rangle$ is an abelian group.
2. $\langle F^*; \cdot \rangle$ is an abelian group where $F^* = F \setminus \{0\}$, "0" is the additive identity.
3. Distributive laws hold.

Theorem 1.3.7. *A finite field with q elements exists if and only if q is a prime power.*

Theorem 1.3.8. *Let F be a field. For $f(x) \in F[x]$, the ring $F[x]/\langle f(x) \rangle$ is a field if and only if $f(x)$ is irreducible over F.*

Proof. Refer to an Algebra Textbook. ∎

Example 1.3.9. Let $F = \mathbb{Z}_2$ and $f(x) = x^2 + x + 1$. Then $f(x)$ is irreducible over $\mathbb{Z}_2$. Hence $\mathbb{Z}_2[x]/\langle x^2 + x + 1 \rangle = \{ax + b + \langle x^2 + x + 1 \rangle \mid a, b \in \mathbb{Z}_2\}$ is a finite field with "4" elements.

$\mathbb{Z}_2[x]/\langle x^3 + x + 1 \rangle$ is a finite field with "8" elements.

$\mathbb{Z}_p[x]/\langle f(x) \rangle$ is a finite field with p^n elements provided (1) $\deg(f(x)) = n$, and (2) $f(x)$ is irreducible over $\mathbb{Z}_2$.

1.4 Orthogonal Latin Square

Definition 1.4.1. Two latin squares $L = [l_{i,j}]$ and $M = [m_{i,j}]$ of order n are *orthogonal* if $\{(l_{i,j}, m_{i,j}) \mid 0 \leq i, j \leq n-1\} = [0, n-1] \times [0, n-1]$, where $[0, n-1]$ denotes the set $\{0, 1, 2, \cdots, n-1\}$.

Example 1.4.2.

0	1	2
2	0	1
1	2	0

$\perp$

0	2	1
2	1	0
1	0	2

Proposition 1.4.3. (Two Fingers' Rule)
$L = [l_{i,j}]$ and $M = [m_{i,j}]$ are orthogonal if for any $0 \leq i, i', j, j' \leq n-1$, $l_{i,j} = l_{i',j'}$ implies that $m_{i,j} \neq m_{i',j'}$.

Proof. By Definition 1.4.1. ∎

Example 1.4.4.

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

$\perp$

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

$\perp$

Three mutually orthogonal latin squares of order 4.

(∗) This example solves the poker cards' problem, published in 1732.

Theorem 1.4.5. *For each prime p and positive integer n, there exist $p^n - 1$ mutually orthogonal latin squares, except when $p = 2$ and $n = 1$.*

Proof. Let F be a finite field of order p^n. Now, for each $k \in F^*$, and $i, j \in [0, p^n - 1]$, let $l_{i,j} = i + kj$. Then, we have $p^n - 1$ latin squares of order p^n. It suffices to prove that these latin squares are mutually orthogonal.

Let $h, k \in F^*$ and $h \neq k$. Assume that $l^{(h)}_{i,j} = l^{(h)}_{i',j'}$ and $l^{(k)}_{i,j} = l^{(k)}_{i',j'}$ where $i \neq i'$ or $j \neq j'$.

Then $i + hj = i' + hj'$, $i + kj = i' + kj'$.

$\Rightarrow (h - k)j = (h - k)j' \Rightarrow j = j'$.

$\Rightarrow i = i'$.

By two fingers' rule, we conclude that $L^{(h)} \perp L^{(k)}$ where $L^{(h)} = \left[l^{(h)}_{i,j}\right]$ and $L^{(k)} = \left[l^{(k)}_{i,j}\right]$. ∎

Definition 1.4.6. (The Kronecker product of two latin squares)

Let $A = [a_{i,j}]_{k\times k}$ and $B = [b_{i,j}]_{h\times h}$ be two latin squares of order k and h respectively. Then, the Kronecker product of A and B, $A \otimes B$ is a $kh \times kh$ latin square defined as follows:

$(a_{0,0}, B)$	$(a_{0,1}, B)$	$\cdots$	$(a_{0,k-1}, B)$
$(a_{1,0}, B)$	$(a_{1,1}, B)$	$\cdots$	$(a_{1,k-1}, B)$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(a_{k-1,0}, B)$	$(a_{k-1,1}, B)$	$\cdots$	$(a_{k-1,k-1}, B)$

where $(a, B) =$

$(a, b_{0,0})$	$(a, b_{0,1})$	$\cdots$	$(a, b_{0,h-1})$
$(a, b_{1,0})$	$(a, b_{1,1})$	$\cdots$	$(a, b_{1,h-1})$
$\vdots$	$\vdots$	$\ddots$	$\vdots$
$(a, b_{h-1,0})$	$(a, b_{h-1,1})$	$\cdots$	$(a, b_{h-1,h-1})$

.

Proposition 1.4.7. If A and B are latin squares, then $A \otimes B$ is also a latin square.

Proof. Directly by definition. ∎

Example 1.4.8. $A =$

0	1	2
1	2	0
2	0	1

, $B =$

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

$A \otimes B =$

00	01	02	03	10	11	12	13	20	21	22	23
01	00	03	02	11	10	13	12	21	20	23	22
02	03	00	01	12	13	10	11	22	23	20	21
03	02	01	00	13	12	11	10	23	22	21	20
10	11	12	13	20	21	22	23	00	01	02	03
11	10	13	12	21	20	23	22	01	00	03	02
12	13	10	11	22	23	20	21	02	03	00	01
13	12	11	10	23	22	21	20	03	02	01	00
20	21	22	23	00	01	02	03	10	11	12	13
21	20	23	22	01	00	03	02	11	10	13	12
22	23	20	21	02	03	00	01	12	13	10	11
23	22	21	20	03	02	01	00	13	12	11	10

xy in $A\otimes$ represents (x, y).

Theorem 1.4.9. *If $A_1 \perp A_2$ and $B_1 \perp B_2$, then $A_1 \otimes B_1 \perp A_2 \otimes B_2$.*

Proof. By two fingers' rule. Assume that $A_1 = \left[a_{i,j}^{(1)}\right], A_2 = \left[a_{i,j}^{(2)}\right], B_1 = \left[b_{i,j}^{(1)}\right], B_2 = \left[b_{i,j}^{(2)}\right]$. Also, let $\left(a_{i,j}^{(1)}, b_{i',j'}^{(1)}\right) = \left(a_{x,y}^{(1)}, b_{x',y'}^{(1)}\right)$ and $\left(a_{i,j}^{(2)}, b_{i',j'}^{(2)}\right) = \left(a_{x,y}^{(2)}, b_{x',y'}^{(2)}\right)$. Now, we have

two cases to consider. First, if $\left(a^{(1)}_{i,j}, b^{(1)}_{i',j'}\right)$ and $\left(a^{(1)}_{x,y}, b^{(1)}_{x',y'}\right)$ are in a subarray (a, B_1) of $A_1 \otimes B_1$ for some $a = a^{(1)}_{i'',j''}$, then $b^{(2)}_{i',j'} \neq b^{(2)}_{x',y'}$ since $B_1 \perp B_2$, a contradiction. On the other hand, if they are in distinct subarrays, (a, B_1) and (a', B_1), then $a^{(2)}_{i,j} \neq a^{(2)}_{x,y}$ since $A_1 \perp A_2$, a contradiction. Hence $A_1 \otimes B_1 \perp A_2 \otimes B_2$. ∎

Proposition 1.4.10. Let $M(n)$ denote the number of mutually orthogonal latin squares of order n. Then, $M(n) \leq n-1$. Moreover, if $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$, then for $n \neq 2, 6$, $M(n) \geq \min\{p_i^{n_i} - 1 \mid i = 1, 2, \cdots, t\}$ (p_i's are distinct primes).

Proof. Observe that if A and B are latin squares of order n such that $A \perp B$, then $\alpha(A) \perp \beta(B)$ for any pair of permutations of $[0, n-1]$. Therefore, if $A_1, A_2, \cdots, A_m$ are mutually orthogonal latin squares of order n, we may let these latin squares have the first row $(0, 1, 2, \cdots, n-1)$. Now, consider the entry at $(1, 0)$ cells. Since $A_1, A_2, \cdots, A_m$ are mutually orthogonal, the corresponding entries at $(1, 0)$-cell must be distinct.(?) So, there are at most $n-1$ of them (distinct from 0). Thus, $m \leq n-1$, i.e., $M(n) \leq n-1$.

For the second part, it follows from $M(p^{n_i}) = p^{n_i} - 1$ whenever p is a prime and the Kronecker product of mutually orthogonal latin squares of order $p_i^{n_i}$, $i = 1, 2, \cdots, t$. ∎

Corollary 1.4.11. *For each positive integer $n > 1$, there exists a pair of mutually orthogonal latin squares of order n provided $n \not\equiv 2 \pmod 4$.*

Euler's Conjecture For each $n \equiv 2 \pmod 4$, there does not exist a pair of orthogonal latin squares.
($*$) The conjecture holds for $n = 2$ and 6 only.
($**$) A counterexample to Euler's conjecture was obtained in Nov. 1959.

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

$\perp$

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

For more constructions of mutually orthogonal latin squares, we shall to it following the idea of pairwise balanced designs.

Exercise 1.4.12. Construct a finite field GF(4) and then use it to construct three mutually orthogonal latin squares.

Exercise 1.4.13. Prove or disprove that for $n \geq 3$ if there are $n-2$ mutually orthogonal latin squares of order n, then there are $n-1$ mutually orthogonal latin squares of order n.

(Note) A set of $n-1$ mutually orthogonal latin squares of order n is called a complete family of orthogonal latin squares.

1.5 Critical Sets

Definition 1.5.1. A *critical set* is a partial latin square of order n which is uniquely completable to a latin square of order n and omiting any entry of the partial latin square destroys the property "uniquely completable".

If a critical set C is uniquely completed to a latin square L, then we also say C is a critical set of L. Clearly, if L is of order n, then the followings hold:

1. $C^{(\alpha)}, C_{(\beta)}$, and $\gamma(C)$ are critical sets of $L^{(\alpha)}, L_{(\beta)}$, and $\gamma(L)$ respectively.
2. C contains at least $n-1$ entries.
3. No two rows or columns of C are empty.
4. The conjugate of C is also a critical set of a latin square (the conjugate of L).

Example 1.5.2. (of critical sets)

0	

0		
	1	

0	1		
1			
			3

0	1	2	3	
1	2	3		
2	3			
3				

We remark here that the well-known game "Sudoku" is very close to use the idea of "critical set" to complete a partial latin square to a latin square with special property: There are nine sub-partial-latin square of order 3 based on $\{1, 2, \cdots, 9\}$.

It is not difficult to see that there are critical sets (of the same order) which are of different sizes, for example both of the following partial latin squares are critical sets. Therefore, it is interesting to know, for a fixed order n what are the sizes of critical sets.

0	1		
1			
			3

0	1	2	
1	2		
2			

Definition 1.5.3. The critical sets of minimum size and maximum size are denoted by $C_r(n)$ and $\tilde{C}_r(n)$.

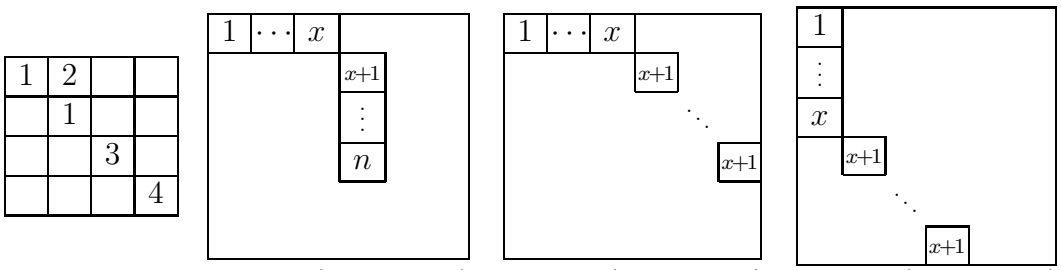
By the example above, we have $C_r(4) \leq 4$ and $\tilde{C}_r(4) \geq 6$.

Conjecture 1.5.4. $C_r(n) \geq \left\lfloor \frac{n^2}{4} \right\rfloor$.

This conjecture is still very far from being settled. The following strong result provides a proof of the fact that for $n \geq 5$, $C_r(n) \geq n+1$.

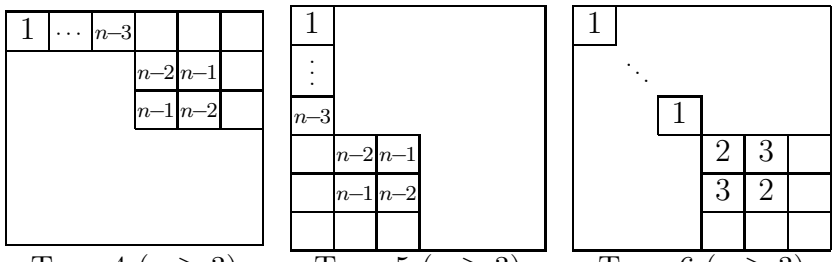
Theorem 1.5.5. (L.D. Anderson)

A partial latin square of order n with size at most $n+1$ can be completed to a latin square if it is not of the following forms (up to isotopism).

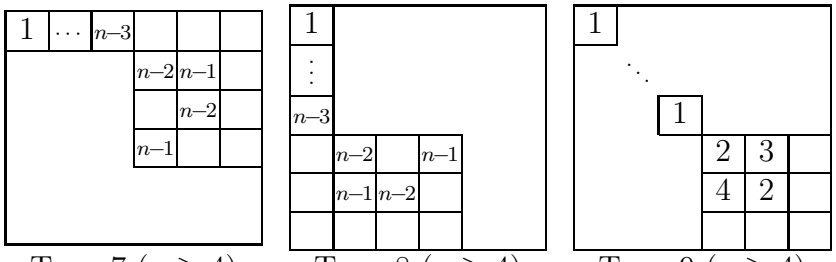


Type 1 ($1 \le x < n$) Type 2 ($1 \le x < n$) Type 3 ($1 \le x < n$)

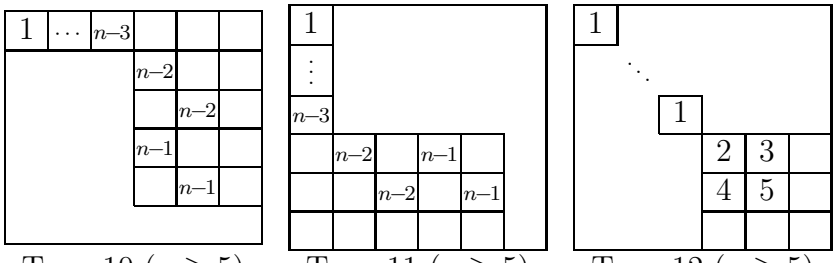
The Noncompletable Partial Latin Squares of Side n with n Nonempty Cells.



Type 4 ($n \ge 3$) Type 5 ($n \ge 3$) Type 6 ($n \ge 3$)



Type 7 ($n \ge 4$) Type 8 ($n \ge 4$) Type 9 ($n \ge 4$)



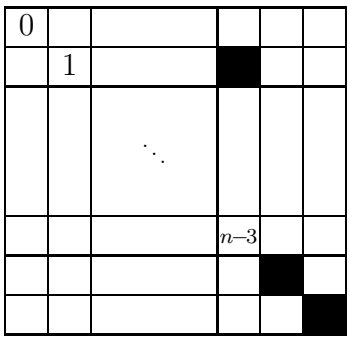
Type 10 ($n \ge 5$) Type 11 ($n \ge 5$) Type 12 ($n \ge 5$)

The Noncompletable Partial Latin Squares of Side n with $n+1$ Nonempty Cells.

Theorem 1.5.6. *$C_r(n) \ge n+1$ for $n \ge 5$.*

Proof. It suffices to prove that there exist no critical sets of size n. Suppose not. Let C be a critical set of size n. By definition and the remarks following the definition we may

assume that C is of the following shape with ■ as undecided entry, two of them must be filled and one of them is $n-2$.



Now, we claim that by adding an arbitrary element to the open ■ left we can complete the partial latin square to a latin square. This is by the fact that this new partial latin square is not of any shapes pointed out in Theorem 1.5.5. Hence, C is not uniquely completed and we have the proof. ■

This result has been improved respectively by Fu and Rodger, and P. Horak later, the new results show that $C_r(n) \geq \lfloor \frac{7n}{6} \rfloor$ for larger n.

It is also worth of mention that the idea of critical set can be applied in secret sharing schemes. The main reason is that we can use mutually orthogonal latin squares to encrypt a message with common "key" a pair of latin squares. Since a latin square can be uniquely determined by its critical set and a part of this critical set is going to be completely to a very large number of distinct latin squares, suitable partition of the critical set provides a sharing scheme. For more information, the readers may refer to the book "Discrete Math. Using Latin Squares" by C. F. Laywine and G. L. Mullen.

1.6 Embedding Partial Latin Squares

It is not difficult to notice that not every partial latin square of order n can be completed to a latin square of order n. But, if we are allowed to add more rows and respectively columns, then it is quite possible to get the job done (completing) as long as enough rows and columns are added.

Definition 1.6.1. (Embedding)

A partial latin square $A = [a_{i,j}]$ of order m based on $\{0, 1, 2, \cdots, n-1\}$ is said to be *embedded* in a latin square $L = [l_{i,j}]$ of order n if for each filled entry $a_{i,j}$, $a_{i,j} = l_{i,j}$. A partial latin rectangle can be defined accordingly.

Example 1.6.2.

A_1 :

0	
	1

L_1 :

0	2	1
2	1	0
1	0	2

A_2 :

0	2
3	1

L_2 :

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

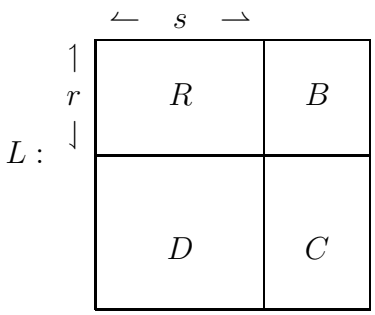
Note When we are dealing with "embedding" both A and L are based on the same set S and if L is of order n then $S = \{0, 1, 2, \cdots, n-1\}$.

Since A is a partial latin square (based on S), not necessarily every element of S occurs in A. The following theorem is an important break through in solving embedding problem.

Theorem 1.6.3. (Ryser's Theorem)

A filled $r \times s$ partial latin rectangle R based on $\mathbb{Z}_n$ can be embedded in a latin square L if and only if $R(i) \geq r + s - n$ when $R(i)$ is the number of occurrence of i in R.

Proof. (Necessity) Let L be as in the following figure.



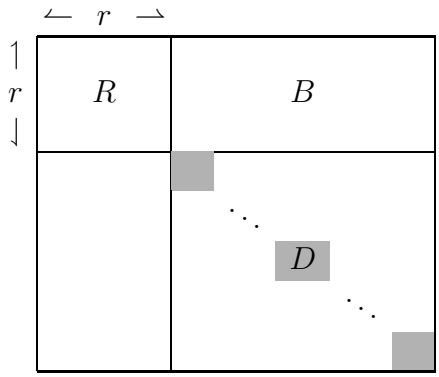
Consider an arbitrary element i. i occurs in B at most $n - s$ times since $B + C$ is a latin rectangle such that each element occurs exactly $n - s$ times. Hence i occurs in R at least $r - (n - s) = r + s - n$ times.

(Sufficiency) By Proposition 1.2.17, it suffices to prove that we can extend R to $R + B$ to obtain an $r \times n$ latin rectangle. First, we define an $r \times n$ $(0, 1)$-array $B^* = [b_{i,j}]$ such that $b_{i,j} = 1$ is and only if j does not occur in the i-th row of R. Then, for each row of B^*, its row sum is equal to $n - s$. Since $R(i) \geq r + s - n = r - (n - s)$, each column sum is at most $r - (r + s - n) = n - s$. Therefore, by Hall's Theorem, B^* can be partitioned into $n - s$ subarrays such that each one of them contains exactly r 1's which are in distinct columns.(?) Then, the proof follows. ∎

Corollary 1.6.4. *A latin square of order m can be embedded in a latin square of order n if and only if $n \geq 2m$.*

If we restrict the type of latin square L, say L is idempotent, then the embedding problem is getting more difficult.

Theorem 1.6.5. *Let $D(i)$ be the number of i occurs in D, see Figure below. Then $R + D$ can be embedded in L if and only if for each $i \in \mathbb{Z}_n$, $R(i) \geq 2r - n + D(i)$.*



D : Part of diagonal.

Proof. Since the sufficiency is not easy to prove, we only prove the necessity part here. Clearly if i occurs in D $D(i)$ times, then i occurs in B at most $n-r-D(i)$ times. Therefore, i occurs in R at least $r-(n-r-D(i))$ times. This concludes the proof. ∎

Corollary 1.6.6. *A partial idempotent latin square of order r can be embedded in an idempotent latin square of order n if and only if (a) for $0 \leq i \leq r-1$, $R(i) \geq 2r-n$ and (b) for $r \leq i \leq n-1$, $R(i) \geq 2r-n+1$.*

Corollary 1.6.7. *An idempotent latin square of order m can be embedded in an idempotent latin square of order n is and only if $n \geq 2m+1$.*

Proof. (Necessity) Since $R(i) = 0$ for each $i \in \{m, m+1, \cdots, n-1\}$, $0 \geq 2m-n+1$ and thus $n \geq 2m+1$.

(Sufficiency) By direct construction.(?) ∎

Note We can use an n-edge-coloring of an n-regular subgraph of $K_{n-m,n-m}$ to obtain the above construction, see it?

Example 1.6.8.

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

The space left is corresponding to a 3-regular subgraph of $K_{6,6}$ which is 3-edge-colorable.

Exercise Prove that an idempotent commutative latin square of order m can be embedded in an idempotent commutative latin square of order n if and only if $n \geq 2m+1$.

1.7 Partial Transversal in a Latin Square

Definition 1.7.1. Let $L = [l_{i,j}]$ be a latin square of order n. A collection of n cells $(i_1, j_1), (i_2, j_2), \cdots, (i_n, j_n)$ is a *transversal* of L provided that

(a) $\forall\ h \neq k$, $i_h \neq i_k$ and $j_h \neq j_k$; and

(b) $\forall\ h \neq k$, $l_{i_h,j_h} \neq l_{i_k,j_k}$.

Definition 1.7.2. A collection of n cells is called a *partial transversal* if only **(a)** satisfies. The number of distinct entries is said to be the *size* of the partial transversal.

Example 1.7.3.

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

A partial transversal of size 3

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

A transversal

Proposition 1.7.4. If L has an orthogonal mate M, i.e., $L \perp M$, then L has n disjoint transversals provided L is of order n.

Proof. For each $i \in \mathbb{Z}_n$, the cells filled with i in M correspond to a transversal in L. ∎

Not every latin square has a transversal.

Proposition 1.7.5. For each singly even integer $2m$ where m is odd, there exists a latin square L of order $2m$ such that L has no transversals.

Proof. Let L be obtained by the Kronecker product of a latin square of order m and $\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array}$. Then it is a routine matter to check that L has no transversals. ∎

Example 1.7.6.

L :

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

$(*)$ If L has a transversal, then at least two distinct elements are from one subsquare. clearly, if we choose three distinct elements from one subsquare, then no way to find a transversal. On the other hand, if two are from left-upper corner, and one from right-lower corner, then we only have one row and one column to choose the other three which is impossible.

Conjecture 1.7.7. (Ryser's Conjecture)
Let L be a latin square of odd order n, then L has a transversal. If L is of even order n, then L has a partial transversal of size $n-1$.

Both parts of the above conjecture remain open (unsettled) which are believed to be very difficult to get the conjecture proved or disproved. In what follows, we use T to denote a maximal partial transversal (with maximum size $|T|$ in a latin square of order n). Then, clearly $|T| \leq n$. It is interesting to know the lower bound. The following result was obtained by D. Woolbright more than 30 years ago, see JCT(A) **24** 235-237, (1978).

Theorem 1.7.8. (D. Woolbright)
$|T| \geq n - \sqrt{n}$.

Proof. Let S be an $n \times n$ latin square. It is well known that S can be represented as an n-edge-coloring of the complete bipartite graph as follows: Let $K_{n,n}$ be the complete bipartite graph with vertex classes $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ and let $c_1, c_2, \ldots, c_n$ be n distinct colors. Color edge (a_i, b_j) with c_k if and only if cell (i, j) in S contains the symbol k. Then a transversal T of S is equivalent to n parallel edges in $K_{n,n}$ and the n parallel edges in $K_{n,n}$ will have $|T|$ distinct colors.

Let T be a transversal in S such that $|T| = t$ is a maximum and let P be the collection of n edges in $K_{n,n}$ that correspond to T. By renaming the vertices in A and B we can assume without loss of generality that $P = \{(a_i, b_i) \mid i \in 1, 2, \ldots, n\}$ and that $\pi = \{(a_i, b_i) \mid i \in 1, 2, \ldots, t\}$ is a collection of t edges with pairwise distinct colorings. Since T was a

transversal of maximal size in S, π is a maximal collection of parallel edges in $K_{n,n}$ with pairwise distinct colorings. We can assume that $c_1, c_2, \ldots, c_{n-t}$ are the colors which do not occur in π.

Let $A_1, A_2, \ldots, A_k$ and $B_1, B_2, \ldots, B_k$ be two sequences of sets of vertices in A and B with the following properties:

(1) $A_1 = \{a_n, a_{n-1}, \ldots, a_{t+1}\}$, and $B_1 = \{b_n, b_{n-1}, \ldots, b_{t+1}\}$,

(2) $A_i \subset A_{i+1}$ and $B_i \subset B_{i+1}$,

(3) $|A_{i+1} \setminus A_i| = |B_{i+1} \setminus B_i| = n - t$,

(4) the $n-t$ edges with vertices in $B_{i+1} \setminus B_i$ which are colored c_i all have vertices in A_i, and

(5) any edge (a, b) such that $a \in A_i$ and $b \in B_1$ is not colored c_j if $i \leq j \leq n - t$.

We claim that if $A_1, A_2, \ldots, A_k$ and $B_1, B_2, \ldots, B_k$ are sequences with properties **(1)**, **(2)**, **(3)**, **(4)**, and **(5)** and if $k < n - t + 1$ then we can always construct sets A_{k+1} and B_{k+1} such that the sequences $A_1, A_2, \ldots, A_k, A_{k+1}$ and $B_1, B_2, \ldots, B_k, B_{k+1}$ also have properties **(1)**, **(2)**, **(3)**, **(4)**, and **(5)**

Since sequences A_1 and B_1 as defined above satisfy properties **(1)**, **(2)**, **(3)**, **(4)**, and **(5)** and therefore can be extended to the sequences $A_1, A_2, \ldots, A_{n-t+1}$ and $B_1, B_2, \ldots, B_{n-t+1}$ satisfying these same conditions. Since $|A_{i+1} \setminus A_i| = n - t$ we have $n \geq (n-t)(n-t+1)$, $n \geq (n-t)^2 + (n-t)$, $n \geq (n-t)^2$, $\sqrt{n} \geq n - t$, $|T| = t \geq n - \sqrt{n}$. This concludes the proof. ∎

As to the search of a larger partial transversal, the following result is the best up to now.

Theorem 1.7.9. (P. Shor)
Every latin square of order n has a partial transversal of size at least $n - (11.053)(\ln n)^2$.

Proof. See JCT(A) **115**(7) 1103-1113, (2008). ∎

In order to improve the above lower bound, a different approach has to be obtained. I believe this is quite possible.

1.8 Special Latin Squares

since a latin square can be obtained from an operation table of a quasigroup, there are quite a few special latin squares which is a direct consequence of special quasigroups, see Lecture Note for a reference. In this section, we shall mainly consider a kind of latin squares that are useful in constructing designs.

Definition 1.8.1. (Latin squares with holes)
Let $\{H_1, H_2, \cdots, H_k\}$ be a partition of $\mathbb{Z}_n$. We say $L = [l_{i,j}]$ is a *latin square with hole-type* $|H_1| \times |H_2| \times \cdots \times |H_k|$ if the following two conditions hold:

(a) $\forall i, j \in H_l$, the cell (i, j) is empty, i.e., we don't assign $l_{i,j}$.

(b) Every element of $\mathbb{Z}_n$ occurs in each row (and each column) at most once and furthermore if $t \in H_l$ for some l, then t does not occur in the t-th row and also t-th column.

the following two partial latin square are latin squares of order 6 and 8 (respectively) with hole-types 2^3 and 2^4 respectively. In fact, both of them are commutative.

		5	6	3	4
		6	5	4	3
5	6			1	2
6	5			2	1
3	4	1	2		
4	3	2	1		

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

Note here that the above two partial squares can be completed to a latin square without any difficulty.

Theorem 1.8.2. *For each even $n \neq 4$, there exists a commutative latin square of order n with hole-type $2^{n/2}$.*

Proof. If $\frac{n}{2}$ is odd, then the construction can be obtained by using the Kronecker product of an idempotent commutative latin square of order $\frac{n}{2}$ and a latin square of order 2. On the other hand, if $\frac{n}{2}$ is even, then we need to use an embedding result obtained earlier by Fu and Fu in [$*$]: If there exists a commutative latin square of order $2m$ with hole-type 2^m, then there exists a commutative latin square of order $2m+4$ with hole-type 2^{m+2}. Since the proof is not a short one, we omit the details. ∎

[$*$] Chin-Mei Fu and Hung-Lin Fu, On the intersection of latin squares with holes, *Utilitas Mathematica* **35** (1989), 67-74.

If we don't need the commutative property, then it is easier to construct a latin square with hole-type l^k for $k \geq 3$. Simply, we use the Kronecker product of an idempotent latin square of order k and a latin square of order l to construct such a latin square.

1.9 Room Squares

This is a type of squares which are very close to the idea of latin squares. Since they are useful in constructing special designs and also cycle systems, we introduce the notion in this section.

Definition 1.9.1. A *room square* of order $2n$ is a $(2n-1) \times (2n-1)$ array based on $\mathbb{Z}_{2n}$ such that each cell is filled with either two elements or empty such that in each row and each column every element of $\mathbb{Z}_{2n}$ occurs exactly once, moreover every pair of distinct elements occurs exactly once.

Example 1.9.2. (Room squares of order 8)

0,1			6,2		5,7	3,4
4,5	0,2			7,3		6,1
7,2	5,6	0,3			1,4	
	1,3	6,7	0,4			2,5
3,6		2,4	7,1	0,5		
	4,7		3,5	1,2	0,6	
		1,5		4,6	2,3	0,7

0,1	5,6	2,4		3,7		
	0,2	6,7	3,5		4,1	
		0,3	7,1	4,6		5,2
6,3			0,4	1,2	5,7	
	7,4			0,5	2,3	6,1
7,2		1,5			0,6	3,4
4,5	1,3		2,6			0,7

Note There does not exist room squares of order 4 and 6.

From the above examples, it is not difficult to see that K_8 has a 7-edge-coloring such that K_8 can be decomposed into 7 perfect matchings such that each perfect matching is multicolored, i.e., each edge of a perfect matching receives a distinct color. The existence of a room square can also be formulated as follows.

Proposition 1.9.3. the existence of a room square of order $2n$ is equivalent to the existence of two idempotent commutative latin squares of order $2n-1$, L_r and L_c, such that

(1) If $L_r(x,y) = L_c(x,y) = \alpha$, then $x = y = \alpha$.

(2) $\forall a \neq b$, $\exists$ at most one cell (x,y) such that $L_r(x,y) = a$ and $L_c(x,y) = b$.

Proof. (Necessity) Let $\tilde{L}$ be a room square of order $2n$. Since permuting rows and columns of a room square gives another room square, we may assume that $\tilde{L}$ has $(0,1),(0,2),\cdots,(0,n-1)$ in its diagonal cells. Now, we are ready to define two latin squares L_r and L_c (based on $\mathbb{Z}_n \setminus \{0\}$ and indexed by $\mathbb{Z}_n \setminus \{0\}$). For $x \neq y \in \mathbb{Z}_n \setminus \{0\}$, let $L_r(x,y) = a$ and $L_c(x,y) = b$ provided that (x,y) occurs in the a-th row and b-th column of $\tilde{L}$; $L_r(x,x) = L_c(x,x) = x$.

(Sufficiency) If L_r and L_c satisfying **(1)** and **(2)**, then we can define a room square by using a reverse order of the proof of necessity. ∎

Example 1.9.4. (Two idempotent commutative latin squares from the first room square of Example 1.9.2.)

1	6	4	3	7	2	5
6	2	7	5	4	1	3
4	7	3	1	6	5	2
3	5	1	4	2	7	6
7	4	6	2	5	3	1
2	1	5	7	3	6	4
5	3	2	6	1	4	7

1	5	2	6	3	7	4
5	2	6	3	7	4	1
2	6	3	7	4	1	5
6	3	7	4	1	5	2
3	7	4	1	5	2	6
7	4	1	5	2	6	3
4	1	5	2	6	3	7

Note The above two latin squares of order 7 is also called a room-pair of the room square of order 8 in Example 1.9.2.

Note The idea of constructing room squares was first mentioned by T. G. Room in 1955.

After years of effort, the following theorem puts up an end of constructing room squares of all even orders except several small orders which are not possible.

Theorem 1.9.5. *For $n \neq 2, 3$, there exists a room square of order $2n$.*

Proof. (Omitted). ∎

Chapter 2

Steiner Triple systems

2.1 Preliminaries

Let V be a nonempty set and $\mathbb{B}$ be a collection of subsets (repeatable) of V. Then $(V, \mathbb{B})$ is a *design*. If for each element of $\mathbb{B}$ is of the same size, then $(V, \mathbb{B})$ is a *block design*. In case that $|V| = v$ and $|B| = b$ for each $B \in \mathbb{B}$, $(V, \mathbb{B})$ is called a (v, k)-design. It is not difficult to see that a graph is a design and a simple graph of order v is a $(v, 2)$-design. Moreover, a binary (block) code can also be "expressed" as a design. For example, if a binary code is of length n and weight k, then the code is an (n, k)-design.

Example 2.1.1. $\{1101000, 0110100, 0011010, 0001101, 1000110, 0100011, 1010001\} \equiv \{\{0, 1, 3\} + i \mid i \in \mathbb{Z}_7\}$ is a $(7, 3)$-design.

Note "Design" and "Code" are similar notions.

We may use an incidence matrix to represent a design by the following way. Let $V = \{a_1, a_2, \cdots, a_v\}$ and $\mathbb{B} = \{B_1, B_2, \cdots, B_b\}$. Then a $(V, \mathbb{B})$ incidence $(0, 1)$-matrix M is defined by $M = [m_{i,j}]_{v \times b}$ where $m_{i,j} = 1$ if and only if $a_i \in B_j$. (Clearly, the corresponding notions on graphs and codes are also of the same setting.) A more practical application of M is on group testing. For nonadaptive algorithms, we may use the B_j's to represent the elements under test and the a_i's to represent the tests. Therefore, the i-th group test (pool) will contain these those elements B_j where $a_i \in B_j$. A bit of reflection, in group testing, we would like to have less rows than columns, i.e., the number of tests is smaller (far) than the number of elements which are under test.

In order to achieve better performance of a design, we need more constraints on a design.

Definition 2.1.2. A design $(V, \mathbb{B})$ is *incomplete* (and complete otherwise) if for each $B \in \mathbb{B}$, $|B| < |V|$, and a design is *balanced* if for each element $v \in V$, v occurs in a fixed (replication) number "r" of blocks (sets in $\mathbb{B}$). For example, in Example 2.1.1, each element occurs in exactly three blocks and thus $r = 3$.

Definition 2.1.3. A design is *pairwise balanced* if every pair of distinct elements occur in the same number of blocks of $\mathbb{B}$.

Note that Example 2.1.1 is also a pairwise balanced block design.

Definition 2.1.4. A block design $(V, \mathbb{B})$ is a *t-design* if every t-subset of V occurs in λ blocks of $\mathbb{B}$, λ is a fixed positive integer. Such a t-design is also denoted by t-(v, k, λ) *design* where $|V| = v$ and $\forall B \in \mathbb{B}$, $|B| = k$.

So, it is not difficult to see Example 2.1.1 provides a 2-(7,3,1) design.

Observation 2.1.5. A 2-(v, k, λ) design exists if and only if the multigraph λK_v can be decomposed into K_k's.

For convenience, a 2-(v, k, λ) design is denoted by a (v, k, λ)-*design*.

Lemma 2.1.6. *In a (v, k, λ)-design we have the following properties:*

1. *$\lambda(v-1)/(k-1)$ is a positive integer.*
2. *$\lambda v(v-1)/k(k-1)$ is a positive integer.*
3. *$\lambda(v-1) \geq k(k-1)$. (Fisher's inequality)*

Proof. The first two properties are easy to see from the view point of graph decomposition, but the third one does need some effort. Since it is a well-known theorem, we omit it here. ∎

Exercise Prove the Fisher's Inequality. (Hint: Prove that M is of rank v.)

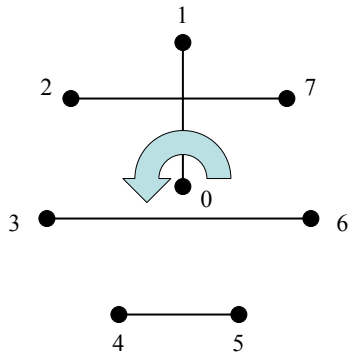
In what follows, we shall focus on the case $k = 3$ and $\lambda = 1$, it is known as the *Steiner triple system*.

2.2 Recursive Constructions

A $(v, 3, 1)$-design is known as the Steiner triple system of order v, denoted by $STS(v)$. By Lemma 2.1.6, it is easy to see that if an $STS(v)$ exists, then $v \equiv 1$ or 3 (mod 6). It was proved in 1847 by T. P. Kirkman that this necessary condition is also sufficient. So far, there are ways of proving this fact. In this section, we first present the well-known *recursive constructions*. We shall also present *direct constructions* in section 3 and *cyclic constructions* in section 4.

Lemma 2.2.1. *The complete graph K_{2m} can be decomposed into $2m-1$ 1-factors, i.e., K_{2m} has a 1-factorization.*

Proof. The following figure ($m = 4$) shows the idea of decomposition. ∎



It is worth of mention that to determine whether a graph has a 1-factorization or not is a very difficult problem.

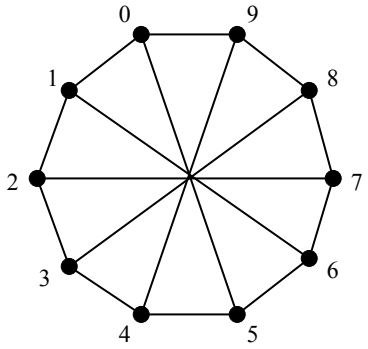
Conjecture 2.2.2. (A. J. W. Hilton) A k-regular graph of order $2n$ has a 1-factorization provides $k \geq n$.

Note This conjecture has been verified for k which is very close to $2n$.

For special graphs, there are excellent results. Before we state the theorem we need to introduce a new notion. Let a graph G of order v defined on $\mathbb{Z}_v$. Then the (*circular*) *difference* of i and j, $i < j$, is defined as $j - i$ if $j - i \leq \lfloor \frac{v}{2} \rfloor$ and $v + i - j$ if $j - i > \lfloor \frac{v}{2} \rfloor$. For example, the difference set of a complete graph defined on $\mathbb{Z}_{11}$ is $\{1, 2, 3, 4, 5\}$ and the difference set of a complete graph defined on $\mathbb{Z}_{10}$ is also $\{1, 2, 3, 4, 5\}$. The key difference between these two examples is that the difference "5" induces a 2-factor in the first graph and a 1-factor in the second one. So, for convenience, if a difference induces a 2-factor is called a *full* difference and *half* difference on the other hand.

Definition 2.2.3. Let $D \subseteq \left\{1, 2, \cdots, \lfloor \frac{v}{2} \rfloor\right\}$. Then $G(D; v)$ is the graph induced by the set of edges $\{\{i, j\} \mid$ the circular difference of i and j is in $D\} = \{\{i, j\} \mid \min\{|i-j|, v-|i-j|\} \in D\}$

Example 2.2.4. $G(\{1, 5\}; 10)$



Clearly, $G(\{1, 5\}; 10)$ has a 1-factorization. It is interesting to know "for which D, $G(D; v)$ has a 1-factorization". The following theorem obtained by Stern and Lenz is a very important break through toward answering the above question.

Theorem 2.2.5. *If D contains an element d where $\frac{v}{\gcd(d,v)}$ is even, then $G(D; v)$ has a 1-factorization.*

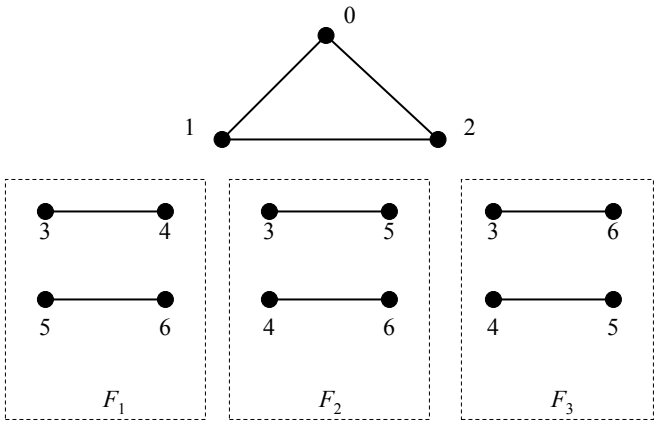
Proof. Refer to the book Design Theory by Chris Rodger and Curt Lindner. ∎

Since v is even when we are considering the existence of 1-factorizations, therefore $G(D; v)$ has a 1-factorization provides there exists a $d \in D$ such that $\gcd(d, v) = 1$ or $\frac{v}{2} \in D$. We shall use the later property in what follows.

Proposition 2.2.6. ($v \to 2v+1$ Construction)
If there exists an $STS(v)$, then there exists an $STS(2v+1)$.

Proof. Let $(\mathbb{Z}_v, \mathbb{B}_1)$ be an $STS(v)$ and $\{F_1, F_2, \cdots, F_v\}$ be a 1-factorization of the complete graph of order $v + 1$ defined on $\{v, v+1, \cdots, 2v\}$. Now, let $\mathbb{B} = \mathbb{B}_1 \cup \{\langle i-1, F_i\rangle \mid i = 1, 2, \cdots, v\}$ where $\langle i-1, F_i\rangle$ is the set of triangles joining $i-1$ to $\frac{v+1}{2}$ edges of F_i. Then, it is a routine matter to check $(\mathbb{Z}_{2v+1}, \mathbb{B})$ is an $STS(2v+1)$. ∎

Example 2.2.7. ($3 \to 7$ construction)

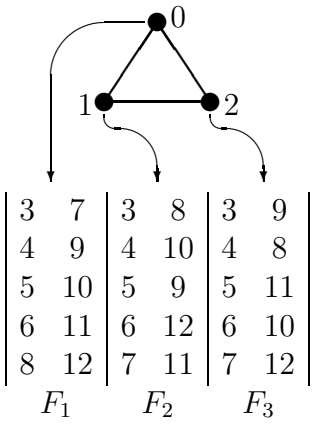


$STS(7) = \{012, 034, 056, 135, 146, 236, 245\}$

Proposition 2.2.8. ($v \to 2v+7$ Construction)
If there exists an $STS(v)$, $v \geq 3$, then there exists an $STS(2v+7)$.

Proof. Let G be the complete graph defined on $\{v, v+1, \cdots, 2v+6\}$. Therefore, G is of order $v+7$. Consider the subgraph $H = G(\{1,2,3\}; v+7)$. Since $v \geq 3$, $G - H = G(D; v+7)$ where $D = \left\{4, 5, \cdots, \frac{v+7}{2}\right\}$ has a 1-factorization $\{F_1, F_2, \cdots, F_v\}$. ($\frac{v+7}{2} \in D$) At the same time, we notice that H can be decomposed into $v+7$ triangles generated by $\{v, v+1, v+3\}$. Now, let $(\mathbb{Z}_v, \mathbb{B}_1)$ be an $STS(v)$ and $\mathbb{B} = \mathbb{B}_1 \cup \{$ triangles from $\{v, v+1, v+3\}\} \cup \{\langle i-1, F_i\rangle \mid i \in \mathbb{Z}_v\}$. Then, $(\mathbb{Z}_{2v+7}, \mathbb{B})$ is an $STS(2v+7)$. ∎

Example 2.2.9. ($3 \to 13$ construction)



$3,4,6$
$4,5,7$
$5,6,8$
$6,7,9$
$7,8,10$
$8,9,11$
$9,10,12$
$10,11,3$
$11,12,4$
$12,3,5$

($*$) F_1, F_2, F_3 are obtained from $G(\{4,5\}; 10)$ defined on $\{3, 4, \cdots, 12\}$.

($*'$) The triangles on left-hand side are obtained from $G(\{1,2,3\}; 10)$ defined on $\{3, 4, \cdots, 12\}$.

Theorem 2.2.10. (Recursive Constructions)
An $STS(v)$ exists if and only if $v \equiv 1$ or $3 \pmod 6$.

Proof. If $v = 12k+3$ or $12k+7$, then by using $v \to 2v+1$ construction we obtain an $STS(v)$. On the other hand, if $v = 12k+1$ or $12k+9$, then an $STS(v)$ can be obtained from $v \to 2v+7$ by letting $v = 6k-3$ and $6k+1$ respectively. This concludes the proof. ∎

2.3 Direct Constructions

We review that a commutative latin square of order $2n$ with hole-type 2^n exists if $n \neq 2$. Also, an $STS(v)$ exists for $v \leq 15$ by direct constructions. Now, we are ready for the main construction.

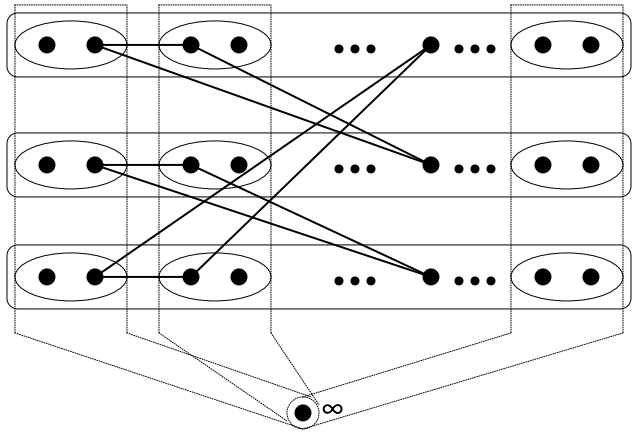
Theorem 2.3.1. (Direct Construction)
An $STS(v)$ exists if and only if $v \equiv 1$ or $3 \pmod 6$.

Proof.
Case 1. $v = 6k + 1, k \geq 3$.

For convenience, let $V = \{\infty\} \cup \{(i, j) \mid i \in \mathbb{Z}_3 \text{ and } j \in \mathbb{Z}_{2k}\}$ and $L = [l_{x,y}]$ be a commutative latin square of order $2k$ (defined on $\mathbb{Z}_{2k}$) with hole-type 2^k. Now, let $\mathbb{B}$ be the collection of the following types of triangles:

1. **Type I**: the triangles in an $STS(7)$ defined on $\{\infty\} \cup \{(i, 2t), (i, 2t+1)\}$ where $t \in \mathbb{Z}_k$.
2. **Type II**: $\{(i, j_1), (i, j_2), (i + 1, l_{j_1,j_2})\}$ where j_1 and j_2 are not in any 2×2 hole of L and $j_1, j_2 \in \mathbb{Z}_{2k}$.

By direct checking, $(V, \mathbb{B})$ is an $STS(v)$.



$6k + 1$ construction

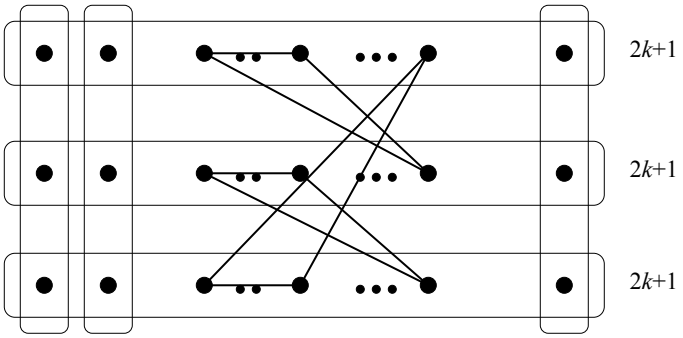
Case 2. $v = 6k + 3, k \geq 3$.

By replacing $\{\infty\}$ in Case 1 with $\{\infty_1, \infty_2, \infty_3\}$ and the **Type I** triangles with the triangles in an $STS(9)$ where $\{\infty_1, \infty_2, \infty_3\}$ is a prescribed triangle, then we have an $STS(v)$. Note here that $\{\infty_1, \infty_2, \infty_3\}$ occurs many times as a **Type I** triangle, but we only let one of them be included. ∎

There are other direct constructions, the one for $6k + 3$ using idempotent commutative latin square of order $2k + 1$ is an excellent construction.

An alternative way to construct $STS(6k+3)$

Instead of using latin squares with hole-type 2^k, we use an idempotent commutative latin square of order $2k+1$. Now, by combining **Type II** triangles mentioned above and the vertical triangles, see the following figure, we have the construction.



$6k+3 = 3 \cdot (2k+1)$ construction

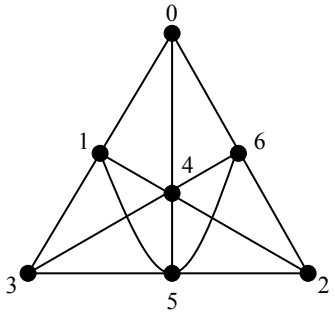
2.4 Cyclic Steiner Triple Systems

Definition 2.4.1. Two block designs $(V_1, \mathbb{B}_1)$ and $(V_2, \mathbb{B}_2)$ are *isomorphic* if there exists a bijection ϕ from V_1 onto V_2 such that $B \in \mathbb{B}_1$ if and only if $\phi(B) = \{\phi(b) \mid b \in B\} \in \mathbb{B}_2$.

Definition 2.4.2. An isomorphism from $(V, \mathbb{B})$ onto itself is called an *automorphism* of $(V, \mathbb{B})$.

Definition 2.4.3. A block design $(V, \mathbb{B})$ is *cyclic* if $(V, \mathbb{B})$ admits an automorphism of order $|V|$.

Example 2.4.4. The Steiner triple system of order 7 (Fano plane) is a cyclic Steiner triple system where $(0, 1, 2, 3, 4, 5, 6)$ is an automorphism.



Fano plane: $\{013, 124, 235, 346, 450, 561, 602\}$.

Definition 2.4.5. In a cyclic block design $(V, \mathbb{B})$, each block generates a set of blocks. If B generates $|V|$ blocks, then the orbit containing B is a *full* orbit and *short* orbit otherwise. A minimum collection of blocks which generate all blocks of $(V, \mathbb{B})$ is called a *basis* of the cyclic design, each block in the basis is a *base-block*.

Example 2.4.6. The following three triples form a basis of a cyclic $STS(15)$: $\{0,1,4\}$, $\{0,2,8\}$, $\{0,5,10\}$. (The last one is a base-block with short orbit and the other two triples are of full orbits.)

From the above example, it is not difficult to see that if a triple $\{x,y,z\}$ is a base-triple, then their (circular) differences a,b,c satisfy one of the following conditions: **(a)** $a+b=c$ or **(b)** $a+b+c=|V|$. In Example 2.4.6, $\{0,2,8\}$ and $\{0,5,10\}$ satisfy **(b)** and $\{0,1,4\}$ satisfies **(a)**. Therefore, in order to construct a cyclic Steiner triple system, we have to arrange (partition) the set of differences into 3-subsets or 1-subsets such that the corresponding base-triples form a basis of the cyclic $STS(v)$. For clearness, we give one more example.

Example 2.4.7. $\{\{0,1,5\},\{0,2,8\},\{0,3,10\}\}$ is a basis of a cyclic $STS(19)$. Note that its difference triples are $\{1,4,5\}$, $\{2,6,8\}$ and $\{3,7,9\}$. In fact, if we consider the difference 9 which is deduced from 10, then we have $3+7=10=_{def}-9$ and thus $3+7+9=19$.

Before we show that a cyclic $STS(v)$ exists for each $v\neq 9$, we introduce a list of useful sequences.

Definition 2.4.8. Let k and n be integers with $1\leq k\leq 2n+1$. A k-extended Skolem sequence of order n is a sequence $(a_1,a_2,\ldots,a_n)$ of n integers such that

$$\bigcup_{i=1}^{n}\{a_i,a_i-i\}=\{1,2,\ldots,2n+1\}\setminus\{k\}.$$

When $k=2n+1$, it is simply called a Skolem sequence of order n.

Example 2.4.9.

1. $(2,5)$ is a 4-extended Skolem sequence of order 2.
2. $(2,7,6,8)$ is a Skolem sequence of order 4.

Definition 2.4.10. Let d,k and n be integers with $n>d$ and $1\leq k\leq 2n+1$. A k-extended Langford sequence of order n and defect d is a sequence $(a_1,a_2,\ldots,a_n)$ of n integers such that

$$\bigcup_{i=1}^{n}\{a_i,a_i-(d+i-1)\}=\{d,d+1,\ldots,d+2n\}\setminus\{d+k-1\}.$$

When $k=2n+1$, it is simply called a Langford sequence of order n and defect d.

Example 2.4.11. $(6,5)$ is a 2-extended Langford sequence of order 2 and defect 2.

Theorem 2.4.12. (Baker, JCD 1995) A k-extended Skolem sequence of order n exists if and only if

1. k is odd and $n\equiv 0,1 \pmod 4$, or
2. k is even and $n\equiv 2,3 \pmod 4$.

Theorem 2.4.13. (Linek and Jiang, JCT(A) 1998) A k-extended Langford sequence of order n and defect 2 exists if and only if

1. k is odd and $n \equiv 0, 3 \pmod 4$, or

2. k is even and $n \equiv 1, 2 \pmod 4$.

Theorem 2.4.14. *A cyclic $STS(v)$ exists for each $v \equiv 1$ or $3 \pmod 6$ except $v = 9$.*

Proof. The exceptional case has been done by checking all permutations in S_9 on the unique $STS(9)$ which is also known as an affine plane of order 3. Let $v \neq 9$.

Case 1. $v = 6k + 1$.

It suffices to find a basis with k base-triples. By Theorem 2.4.12, if $k \equiv 0$ or 1, we can partition $\{k+1, k+2, \cdots, 3k\}$ into k ordered pairs $(a_1, b_1), (a_2, b_2), \cdots, (a_k, b_k)$ such that $b_i - a_i = i$ for $i = 1, 2, \cdots, k$. This implies that the k difference triples are $\{\{i, a_i, b_i\} \mid i = 1, 2, \cdots, k\}$. On the other hand, if $k \equiv 2$ or 3, then we can partition $\{k+1, k+2, \cdots, 3k-1, 3k+1\}$ into k ordered pairs as above and the k difference triples can be obtained accordingly.

Case 2. $v = 6k + 3, k > 1$.

We shall partition $\{k+1, k+2, \cdots, 3k+1\} \setminus \{2k+1\}$ into k ordered pairs (a_i, b_i), $i = 1, 2, \cdots, k$, such that $b_i - a_i = i$. (This is equivalent to partition $\{1, 2, \cdots, k, k+2, \cdots, 2k+1\}$). Since $k+1$ is odd if $k \equiv 0 \pmod 4$ and $k+1$ is even if $k \equiv 3 \pmod 4$, the partition can be done by using Theorem 2.4.12 again. On the other hand, if $k \equiv 1$ or $2 \pmod 4$, then we may partition $\{1, 2, 3, \cdots, k, k+1, \cdots, 2k, 2k+2, \cdots, 3k, 3k+2\}$ into k difference triples[1] and the proof follows. ∎

Remark 1. Cyclic Steiner triple systems of all orders except 9 were constructed by R. Peltesohn in 1939 (Compositio Math., 6). At that time, Skolem sequences did not appear yet. Therefore, Peltesohn constructed all the base triples by the following way:

1. Find a cyclic $STS(v)$ for $v = 7, 13, 15, 19, 27, 45, 63$ directly.

2. Consider the cases by using modulo 18 and thus there are 6 different cases to be done.

Remark 2. Skolem-type of sequences have a large range of applications especially when "cyclic" becomes an important issue.

2.5 Kirkman Triple Systems

Kirkman triple systems are named after Rev. T. P. Kirkman who in 1850 posed and solved the "Kirkman school girl problem": Is that possible for a school mistress to take 15 school girls on a walk each day of the 7 days of a week, walking with 5 rows of 3 girls each, such that each pair of girls walks together in the same row on exactly one day? The answer obtained then is as follows: (π_i for the i^{th} day.)

π_1			π_2			π_3			π_4			π_5			π_6			π_7		
1	2	3	1	4	5	1	6	7	1	8	9	1	10	11	1	12	13	1	14	15
4	8	12	2	8	10	2	9	11	2	12	15	2	13	14	2	4	6	2	5	7
5	10	14	3	13	15	3	12	14	3	5	6	3	4	7	3	9	10	3	8	11
6	11	13	6	9	14	4	10	15	4	11	14	5	9	12	5	11	15	4	9	13
7	9	15	7	11	12	5	8	13	7	10	13	6	8	15	7	8	14	6	10	12

[1]These triples are named Rosa triples which can be referred to:
A. Rosa, Mat. Fyz. Časopis 16 (1966), 285-290.

Definition 2.5.1. (Parallel Class)

A *parallel class* in a Steiner triple system $(V, \mathbb{B})$ is a set of disjoint triples in $\mathbb{B}$ such that their union is V. A *partial* parallel class in $(V, \mathbb{B})$ is a set of disjoint triples in $\mathbb{B}$.

Definition 2.5.2. (Kirkman Triple Systems)

A *Kirkman triple system* $(V, \mathbb{B})$ denoted by $KTS(v)$ is a Steiner triple system $STS(v)$ such that $\mathbb{B}$ can be partition into $\frac{v-1}{2}$ parallel classes.

Clearly, if $(V, \mathbb{B})$ is a $KTS(v)$, then $v \equiv 3 \pmod 6$. The following outstanding result was proved in 1971 by D. K. Ray-Chaudhuri and R. M. Wilson. Since they used pairwise balanced designs with block sizes $\{4, 7, 10, 19\}$, the proof is omitted here.

Theorem 2.5.3. *For each $v \equiv 3 \pmod 6$, there exists a $KTS(v)$.*

Now, a quick question about (partial) parallel classes.

Problem 2.5.4. Given an $STS(v)$, can we partition the set of triples into v partial parallel classes?

Observe that we need 7 partial parallel classes to partition the set of triples in an $STS(7)$ since any two of them have an element in common. Clearly, if the given $STS(v)$ is a $KTS(v)$, then only $\frac{v-1}{2}$ (partial) parallel classes are needed.

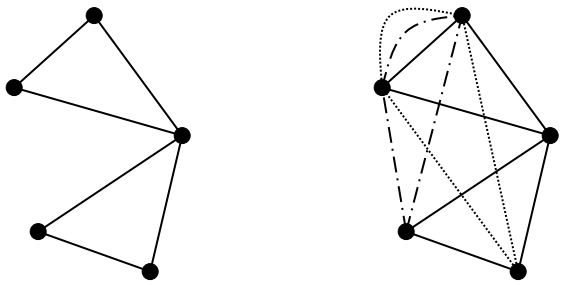
Conjecture 2.5.5. (P. Erdös)

If $(V, \mathbb{B})$ is a design such that any two blocks have at most one element in common, then $\mathbb{B}$ can be partitioned into $|V|$ partial parallel classes (collections of mutually disjoint blocks).

2.6 Packing and Covering a Graph with Triangles

From graph point of view, the existence of an $STS(v)$ is equivalent to the existence of a partition of the edge set of K_v into triangles. For simplicity, we say "K_v can be decomposed into K_3's" and denote it by $K_3 \mid K_v$ or $C_3 \mid K_v$. Clearly, we notice that if $v \not\equiv 1, 3 \pmod 6$, then $K_3 \nmid K_v$. In that case, how many K_3's can we get from K_v? Or, on the other direction, how many K_3's do we need to cover all edges of K_v?

Example 2.6.1. There are at most two triangles (edge-disjoint) in K_5 and we need 4 triangles to cover all edges of K_5, see the following figures.



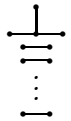
Definition 2.6.2. (Maximum Packing of K_v with Triangles, $MPT(v)$)

The collection of triangles (with largest size) we can obtain from K_v is said to be the *maximum packing* of K_v with triangles, denoted by $MPT(v)$. The subgraph left after taking away the triangles is call the *leave* L of the packing. (Maximum packing has a minimum leave.)

Clearly, the maximum packing of K_v has a leave an empty graph if and only if $v \equiv 1$ or 3 (mod 6).

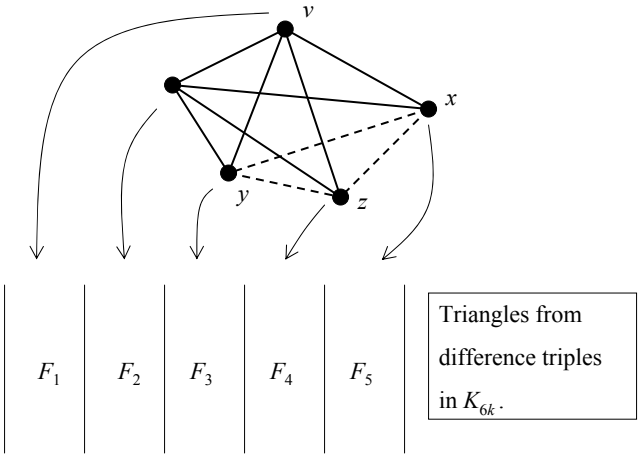
Theorem 2.6.3. *The minimum leaves of maximum packings of K_v are as following table:*

v mod 6	0	1	2	3	4	5
Leave	F	$\emptyset$	F	$\emptyset$	T	C_4

where F is a 1-factor and T is  .

Proof. We start with the case when $v \equiv 0$ or 2 (mod 6). Since K_v is an odd graph, i.e., every vertex is of odd degree, the leave L of any packing of K_v must be an odd graph and therefore L has at least $\frac{v}{2}$ edges. This implies that if there is a packing of K_v with leave F, then the packing is a maximum packing. Indeed, we have such a packing by deleting one vertex from an $STS(v+1)$. This concludes the proof of these two cases.

Now, consider $v \equiv 5$ (mod 6). Since $\|K_v\| \equiv 1$ (mod 3), the leaves of packings are of size $3t+1$ for integers $t \geq 0$. Clearly, $t \neq 0$ since the leave must be an even graph (?). Therefore, if we can find a packing with a leave of size 4, then the packing is a maximum packing. We claim C_4 is the leave we need. By Example 2.6.1, it is true for $v = 5$. First, we show that there exists a packing of K_{6k+5}, $k \geq 1$, such that K_5 is a leave. (Then by taking two triangles away from K_5, we have the desired leave.) Now, consider K_{6k}. The difference set is $\{1, 2, \cdots, 3k\}$ where $3k$ is a half-difference. By using the idea of difference triples as mentioned in Section 2.4, we find $k-1$ difference triples in $\{1, 2, \cdots, 3k\}$ without using $3k$. Hence we have two full-differences and one half-difference left. By Theorem 2.2.5, the subgraph induced by the three differences has a 1-factorization which contains five 1-factors. Now, we have the packing which contains all triangles from $k-1$ difference triples and five collections of triangles obtained from joining five vertices of K_5 to five 1-factors respectively.



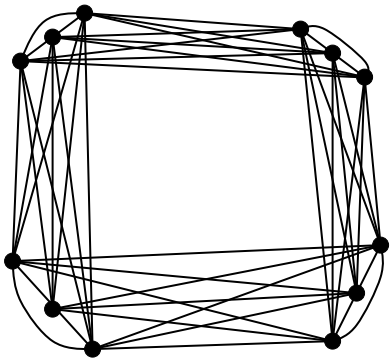
Finally, we consider the case $v = 6k+4$. This can be done by taking away one vertex v of a maximum packing of K_{6k+5} where v is depicted in the figure (above) and one triangle $\{x, y, z\}$. ∎

A natural problem raised from the idea of leaves (remainder graphs): For which kind of L, $K_3 \mid K_v - L$? Of course, we shall assume that $K_v - L$ (3-sufficient) is an even graph with size a multiple of 3.

Conjecture 2.6.4. If L is a spanning odd forest, then $K_3 \mid K_v - L$ provides $K_v - L$ is 3-sufficient.

Conjecture 2.6.5. If $\Delta(L) \leq \frac{1}{4}(v-1)$ and $K_v - L$ is 3-sufficient, then $K_3 \mid K_v - L$.

The following example shows that $\Delta(L) \leq \frac{1}{4}(v-1)$ is necessary (in some sense). The graph $K_{12} - L$ can not be decomposed into triangles. (?)



$$L = K_{3,3} \cup K_{3,3},\ \Delta(L) = 3$$

Exercise 2.6.6. Let L be a spanning odd forest of K_{2m} with $\Delta(L) \leq 3$. Prove that $K_{2m} - L$ can be decomposed into triangles if $K_{2m} - L$ can be decomposed into triangles if $K_{2m} - L$ is 3-sufficient.

Now, we turn to the covering of graphs with triangles.

Definition 2.6.7. A *covering* of a graph G with triangles is a collection of triangles such that their union contains each edge of G at least once. The covering with minimum number of triangles is called a *minimum* covering and the graph induced by the set of edges added to G is called the *padding* (minimum) of the covering (minimum).

Theorem 2.6.8. *The minimum covering of K_v with triangles has paddings as in the following table:*

v mod 6	0	1	2	3	4	5
Padding	F	$\emptyset$	T	$\emptyset$	T	D

where D is $\bigcirc$ and F, T are the same as in packings.

Proof. Exercise. (We may use two vertices ∞_1 and ∞_2 and the leave obtained in K_{v-2} to obtain the padding of K_v.) ∎

2.7 Embeddings of Steiner Triple Systems

The triple system $(V_1, \mathbb{B}_1)$ is said to be embedded in the triple system $(V_2, \mathbb{B}_2)$ provided that $V_1 \subseteq V_2$ and $\mathbb{B}_1 \subseteq \mathbb{B}_2$. It is easy to see that if $(V_1, \mathbb{B}_1)$ is a proper subsystem of $(V_2, \mathbb{B}_2)$, then $|V_2| \geq 2|V_1|+1$. The following theorem is well-known as the **Doyen-Wilson Theorem**.

Theorem 2.7.1. *Let $2u+1 \leq v$, $u \equiv 1$ or $3 \pmod 6$, and $v \equiv 1$ or $3 \pmod 6$. Then there exists an $STS(v)$ containing an $STS(u)$.*

Note The proof of this theorem can be found in Discrete Math. 5 (1973), 229-239. We give another proof here.

Before we prove the theorem, we present a lemma which is also known. You should be able to prove it yourself. (Ex.)

Lemma 2.7.2. *Let $v \geq 3$. Then $G(\{1,2\}; v)$ contains a prescribed 2-factor and a Hamilton cycle.*

Corollary 2.7.3. *If $v \equiv 0 \pmod 3$, then $G(\{1,2\}; v)$ contains a parallel class of triangles and a Hamilton cycle.*

Proof of the Doyen-Wilson Theorem (Outline)

We consider the following cases.

(a) $u \equiv 1 \pmod 6$ and $v \equiv 3 \pmod 6$; $u \equiv 3 \pmod 6$ and $v \equiv 1 \pmod 6$.
Let $u = 6k+1$ and $v = 6h+3$. Then K_{v-u} can be induced by the set differences $D = \left\{1, 2, \cdots, \frac{v-u}{2}\right\}$. since $v-u = 6(h-k)+2$, D has $3(h-k)$ full difference and one half difference. Moreover, by the fact that $3(h-k) \geq 3k$, we may partition D into $h-2k$ difference triples and a set D' which is a set of $3k$ full difference and one half differences. Now, by Stern and Lenz's theorem, K_{v-u} can be partitioned into $6k+1$ 1-factors and a collection of triangles. Hence, by the idea used in recursive constructions we have $K_v \supseteq K_u$. On the other hand, if $u = 6k+3$ and $v = 6h+1$, then $K_{v-u} = K_{6(h-k)-2}$ which can be decomposed into $6k+3$ 1-factors and a collection of triangles induced by $h-2k-1$ difference triples by a similar idea.

(b) $u \equiv 1 \pmod 6$ and $v \equiv 1 \pmod 6$
Let $u = 6k+1$ and $v = 6h+1$. Then K_{v-u} can be partitioned into (i) $6k+1$ 1-factors where two of them are from the Hamilton cycle obtained in $G(\{1,2\}; v-u)$ (Coro. 2.7.3); (ii) $2h-4k-2$ collections of triangles obtained from difference triples; and (iii) a collection of triangles from difference $2(h-k)$ and a parallel class from Coro. 2.7.3. (?)

(c) $u \equiv 3 \pmod 6$ and $v \equiv 3 \pmod 6$.
Let $u = 6k+3$ and $v = 6h+3$. Then K_{v-u} can be partitioned into $6k+3$ 1-factors, triangles from difference triples and the single difference $2(h-k)$. This concludes the proof. ∎

Example 2.7.4. We use three examples to explain the above proof respectively for three cases.
Case 1. $13 \to 63$

(1) $D = \{1, 2, \cdots, 25\}$, $k = 2, h = 10$.

(2) Difference triples ($h-2k = 6$) from $\{1, 2, \cdots, 17, 19\}$ (using Skolem sequence).

(3) Differences left $D' = \{18, 20, 21, 22, 23, 24, 25\}$. ($G(D'; 50)$ has a 1-factorization with 13 1-factors.)

Case 1'. $15 \to 61$

(1) $D = \{1, 2, \cdots, 23\}$, $k = 2, h = 10$.

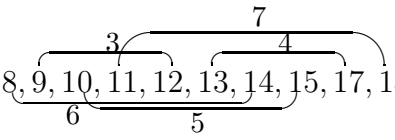
(2) Difference triples ($h-2k-1 = 5$) from $\{1, 2, \cdots, 15\}$.

(3) $D' = \{16, 17, 18, 19, 20, 21, 22, 23\}$ (15 1-factors).

Case 2. $13 \to 61$

(1) $D = \{1, 2, \cdots, 24\}$, $k = 2, h = 10$.

(2) Difference triples (5) from $\{3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 17, 18\}$ (sequences with defect).



(3) Triangles from $G(\{1, 2\}; 48)$ (Corollary. 2.7.3) and the difference 16.

(4) 1-factorization of the union of Hamilton cycle from $G(\{1, 2\}; 48)$ and the set of differences $\{19, 20, 21, 22, 23, 24\}$.

Case 3. $15 \to 63$

(1)+(2)+(4) $D' = \{1, 2, 19, 20, 21, 22, 23, 24\}$.

2.8 λ-fold triple systems

If we consider a triple system such that each pair of distinct elements occur together in exactly $\lambda > 1$ triples, then we have a λ-fold triple system. The existence of such a triple system of order v is equivalent to the existence of a decomposition of λK_v into K_3's where λK_v denotes the complete graph of order v with multiplicity (edge) λ. Therefore the following lemma is easy to see.

Lemma 2.8.1. *If a λ-fold triple system of order v exists, then* ***(a)*** $2 \mid \lambda(v-1)$ *and* ***(b)*** $3 \mid \lambda v(v-1)/2$.

From a simple calculation, we have the following table to depict the spectrum of the existence of a λ-fold triple system.

$\lambda_{>0}$ \ v	0	1	2	3	4	5
0	②	①	④	①	②	③
1	×	①	×	①	×	×
2	②	①	×	①	②	×
3	×	①	×	①	×	③
4	②	①	×	①	②	×
5	×	①	×	①	×	×

(mod 6) (mod 6)

×: Impossible cases.
ⓘ: By i^{th} construction in the followings.

We may prove that all possible cases can be constructed.

Theorem 2.8.2. *A λ-fold triple system of order v exists if and only if* ***(a)*** $2 \mid \lambda(v-1)$ *and* ***(b)*** $3 \mid \lambda v(v-1)/2$.

Proof. ($\Rightarrow$) By direct counting, we have the above table.
($\Leftarrow$) ① Since an $STS(v)$ exists if and only if $v \equiv 1$ or $3 \pmod 6$, we may use λ $STS(v)$ to obtain a desired λ-fold triple system of order v.

② It suffices to consider $\lambda = 2$ and then use copies of a 2-fold triple system of order v to duplicate a λ-fold (λ even) triple system of order v.
$3k$-construction ($k \neq 2$)

We review that an $STS(6k+3)$ can be constructed by using tripling construction with the existence of an idempotent commutative latin square of order $2k+1$. Now, by replacing this latin square with an idempotent latin square of order $k(\neq 2)$, we have a 2-fold triple system of order k, see it?
$3k+1$-construction

Similarly, since a 2-fold triple system of order 4 exists, we may use a $(3k+1)$-construction to obtain a 2-fold triple system of order $3k+1$ by using an idempotent latin square of order k.

Combining the above two constructions and the existence of a 2-fold triple system of order 6 (direct construction), we have ②.

③ This construction can be obtained by showing the existence of a 3-fold triple system of order 5. (K_{6k+5} can be decomposed into triangles and a K_5.)

④ Note that this case excludes $v = 2$ and it suffices to consider the case $\lambda = 6$. Let L be an idempotent latin square of order v. Then, let $V = \mathbb{Z}_v$ and $\mathbb{B} = \{\{a, b, c\} \mid a, b, c \in \mathbb{Z}_v$ and $L(a, b) = c\}$. Clearly, there are $v(v-1)$ triples in $\mathbb{B}$. Moreover, each pair of distinct elements x and y occurs together in a triple exactly 6 times, since we have $x \circ y = z_1, x \circ z_2 = y, z_3 \circ x = y, y \circ z_4 = x, z_5 \circ y = x$ and $y \circ x = z_6$. ("$\circ$" is the corresponding operation in L.)

∎