8 Combinatorial Designs

8.1 Orthogonal Latin Squares

The concept of the latin square probably originated with problems concerning the movement and disposition of pieces on a chess board. The other source of this idea may have been considered in ancient China when the magic sequare was constructed. However, the earliest written reference to the use of such squares known today is the so-called "16 court cards problem".

16 Court Cards Problem

Can we place 16 court cards of Bridge inside a 4×4 grid such that each row, column and diagonal contain exactly one card of each suit and one card of each rank.

It takes not much time to find a solution for this problem, see Figure **??**.

A_S	K_H	Q_D	J_C
Q_C	J_D	A_H	K_S
J_H	Q_S	K_C	A_D
K_D	A_C	J_S	Q_H

S : Spade
H : Heart
D : Diamond
C : Club

Figure 8.1: Arrangement of 16 cards.

An enumerative solution to the problem was published in 1725.[6] But, the most famous problem of similar type is "36 officers problem" proposed by Euler in 1779[LE].

36 Officers Problem

Can we arrange 36 officers of six different ranks and regiments in a square phalanx such that each row and column contain exactly one officer from each rank and one officer from each regiment respectively.

Though this problem turns out to be an impossible mission, the study of latin squares and combinatorial design becomes an interesting topic to mathematicians (combinatorists).

Definition 8.1.1. 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 in 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 8.1.2.

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 $L(\alpha, \beta, \gamma)$.

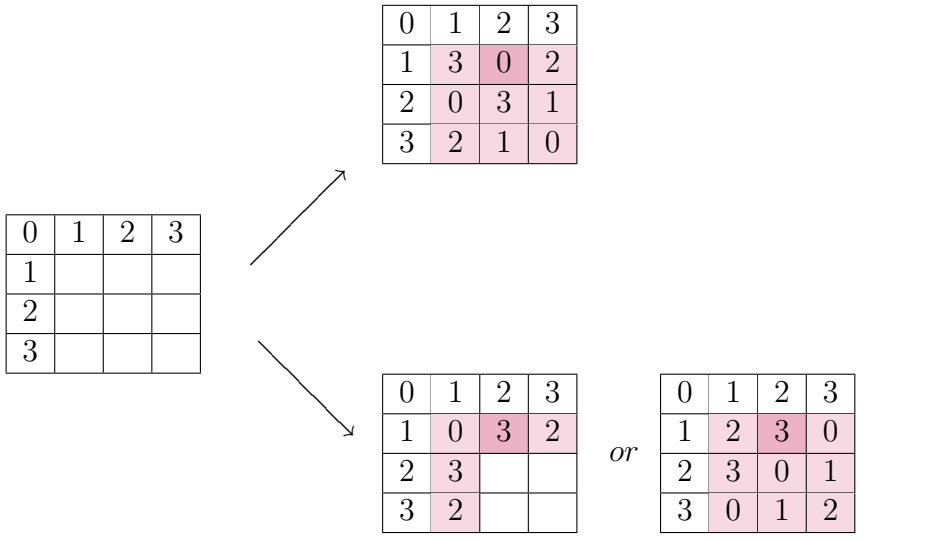
Definition 8.1.3. A latin square $L = [l_{i,j}]$ of order n is said to be a *standard* latin square(or reduced latin square) if $l_{i,0} = i$ and $l_{0,j} = j$ where the rows and columns are indexed by $0, 1, 2, \cdots, n-1$.

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

Proposition 8.1.4. $L_1 = \ell_1 = 1$, $L_2 = 2$ and $\ell_2 = 1$, $L_3 = 12$ and $\ell_3 = 1$, $L_4 = 576$ and $\ell_4 = 4$.

Proof.

0	1	2
1		
2	?	



□

Proposition 8.1.5. $L_n = n!(n-1)!\ell_n$.

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 8.1.6. 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) $1.5 \cdot 10^{86}$, $L_{15} \approx 15! \cdot 14! \cdot 1.5 \cdot 10^{86}$.

Example 8.1.7. Find the number of distinct latin squares of order 9 which are corresponding to all the possible solutions of "Sudoku".(Difficult!)

Definition 8.1.8. 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 8.1.9. 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 $\langle S; \dots \rangle$.

Definition 8.1.10. If $\circ$ is a binary operation on S, then $\langle S; \circ \rangle$ is a *groupoid*.

Definition 8.1.11. 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 8.1.12. 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 8.1.13. 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 obatin 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 8.1.14. 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 *inempotent* 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 arbitary.

Proposition 8.1.15. 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 8.1.16. 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 8.1.17. 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 element, 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 $6 \mid n^2 - n$. 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 section.

Definition 8.1.18. A *latin subsqure* 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 $L = [i_{i,j}]_{n\times n}$, $A = [a_{i,j}]_{m\times m}$ and $m \leq n$.

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

$(*5)$ $m \mid n$ 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 8.1.19. 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 8.1.20. If A is a subsquare of L, we also call A is *embedded* in L.

Definition 8.1.21. 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 8.1.22. Let $m \leq n$. 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 8.1.23.

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 latin rectangle.

Proposition 8.1.24. Every $m \times n$ latin rectangle with $m \leq n$ can be extended to a latin square of order n.

Before we prove this proposition, we review the notion of SDR.[10]

Definition 8.1.25. (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 $1 \leq i < j \leq n$. The following theorem by P.Hall(1935) is well-known. For clearness, we include a proof here.

Theorem 8.1.26. (Hall's Condition)[10]

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

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 $\{A_{h+1} \backslash A, A_{h+2} \backslash A, \cdots, A_{n+1} \backslash A\}$. Since, $h \leq n$, this is not an empty collection. Moreover, let (W.L.O.G.) $A_{h+1} \backslash A, A_{h+2} \backslash A, \cdots, A_{h+k} \backslash A$ be any collection of k sets. Then, $\bigcup_{i=1}^{k} A_{h+i} \backslash A =$

$\bigcup_{i=1}^{k}(A_{h+i} \cap A') = A' \cap \left(\bigcup_{i=1}^{k} A_{h+i}\right)$ 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, $\{A_{h+1}\backslash A, A_{h+2}\backslash A, \cdots, A_{n+1}\backslash A\}$ 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 8.1.24.

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 8.1.27. 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. Use the idea of an SDR.(Exercise) □

Definition 8.1.28. 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 8.1.29.

0	1	2
2	0	1
1	2	0

$\perp$

0	2	1
2	1	0
1	0	2

Proposition 8.1.30. (Two Finger's 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 **??** □

Example 8.1.31.

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

$\perp$

Figure 8.2: Three mutually orthogonal latin squares of order 4

$(*)$ This example solves the poker cards' problem, published in 1723.

Theorem 8.1.32. 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 $i^{(h)}_{i,j} = l^{(h)}_{i',j'}$ 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 prop **??**, we conclude that $L^{(h)} \perp L^{(k)}$ where $L^{(h)} = \left[l^{(h)}_{i,j}\right]$ and $L^{(k)} = \left[l^{(k)}_{i,j}\right]$. $\square$

Definition 8.1.33. (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:

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

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

Proof. Directly by definition. □

Example 8.1.35.

$$A = \begin{array}{|c|c|c|}\hline 0 & 1 & 2 \\ \hline 1 & 2 & 0 \\ \hline 2 & 0 & 1 \\ \hline \end{array}, \quad B = \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline \end{array}$$

$A \otimes B =$

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 $A \otimes B$ represents (x, y).

Theorem 8.1.36. 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 finger's 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 $\left(a_{i,j}^{(1)}, b_{i',j'}^{(1)}\right)$ and $\left(a_{x,y}^{(1)}, b_{x',y'}^{(1)}\right)$ are in a subarray (a, B_1) of $A_1 \otimes B_1$ for some $a = a_{i'',j''}^{(1)}$, then $b_{i',j'}^{(2)} \neq b_{x',y'}^{(2)}$ 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 $a_{i,j}^{(2)} \neq a_{x,y}^{(2)}$ since $A_1 \perp A_2$, a contradiction. Hence $A_1 \otimes B_1 \perp A_2 \otimes B_2$. □

Proposition 8.1.37. 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 $n \neq 2, 6$, $M(n) \geq \min\{p_i^{n_i} - 1 \mid i = 1, 2, \ldots, t\}$ (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 $(0, 1)$-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 8.1.38. 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 square.
($*$) The conjecture holds for $n = 2$ and 6 only.
($**$) A counterexample to Euler's conjecture was obtained in Nov. 1960[2].

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 do it using the idea of pairwise balanced designs.

Exercise 1. Construct a finite field GF(4) and then use it to construct three mutually orthogonal latin squares.

Exercise 2. 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.

8.2 Block Designs

The study of the incidence structures between finite sets is one of the most important topics in Combinatorial theory. There are three basic directions: (1) Finite Geometry, (2) Block Design, and (3) Hypergraph. It is not easy to describe the difference between them. In general, "Finite Geometry" cares more about the property related to the geometry on a plane, "Block Design" emphsizes on numberical relationship and "Hypergraph" focuses on arbitraily given edges (finite subsets).

Therefore, to study Block Design, we start with the construction of designs of small order. We also find the necessary conditions for the existence of the kind of designs we would like to obtain. Following that, we then put forth to prove the necessary conditions are also sufficient by constructing all

such designs. In general, the part on necessary conditions is comparatively easier. As to construction part, some of the design does not exist even we know the necessary conditions. We shall see that in next section.

Definition 8.2.1. $(X, \mathbb{B})$ is a design if X is a non-empty set and $\mathbb{B}$ is a collection of subsets of X. If all the subsets are of the same cardinality, then $(X, \mathbb{B})$ is call a block design. For convenience, all the set in $\mathbb{B}$ are referred as a block in X.

Definition 8.2.2. If all the subsets of a design $(X, \mathbb{B})$ are all distinct, then it is a simple design. Note that $\mathbb{B}$ can be a multi-set in a design, the blocks with repeated occurrence is known as repeated blocks.

Let $X = \{x_1, x_2, \cdots, x_v\}$ be the set of "varieties" and $\mathbb{B} = \{B_1, B_2, \cdots, B_b\}$ be the set of blocks. Then, we can define a Variety-Block incidence matrix to represent the design, say A and also a bipartite graph to represent $(X, \mathbb{B})$, say $G_{X,\mathbb{B}}$.

Here they are:

(1) $A = [a_{i,j}]_{v \times b}$ where $a_{i,j} = \begin{cases} 1, & \text{if } x_i \in B_j, \text{and} \\ 0, & \text{otherwise.} \end{cases}$

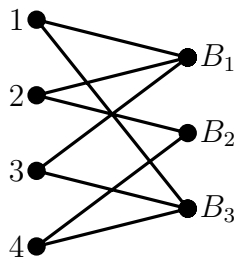
Therefore, A is a $(0,1)$-matrix.

(2) $G_{X,\mathbb{B}} = (X, \mathbb{B})$ is a bipartite graph such that $x_i \sim B_j$ if $x_i \in B_j$.

Example 8.2.3. $X = \{1,2,3,4\}$, $\mathbb{B} = \big\{\{1,2,3\}, \{2,4\}, \{1,3,4\}\big\}$. ($B_1, B_2, B_3$ respectively)

$$A: \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} B_1 & B_2 & B_3 \end{array} \\ \left[\begin{array}{ccc} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right]_{4\times 3} \end{array}$$

$G_{X,\mathbb{B}}$:



Note that the relation of A and $G_{X,\mathbb{B}}$ is easy to see. In coding theory the elements is $\mathbb{B}$ can be referred as the support of codewords. In graph theory,

they are "hyperedges". From the sense of Geometry, the incidence relation $x_i \in B_j$ can be "reversed". We can say "a point x_i is *on* a line B_j " or "a line B_j is *passing* x_i". Hence, we have the following.

Definition 8.2.4. $(\mathbb{B}, X)$ is a dual design of $(X, \mathbb{B})$. The incidence matrix of $(\mathbb{B}, X)$ is A^T where A is the incidence matrix of $(X, \mathbb{B})$.

In an $(X, \mathbb{B})$, we let $r(x)$ or r_x denote the replication number of a variety x, i.e., the number of blocks containing x. We use K to denote $\big\{|B| \,\big|B \in \mathbb{B}\big\}$. If $K = \{k\}$, then we simply use k to denote K.

Definition 8.2.5. A $t-(v, k, \lambda)$ design is an $(X, \mathbb{B})$ such that $|X| = v$, $K = \{k\}$ and any t-subset of $\binom{X}{t}$ occurs together in exactly λ blocks of $\mathbb{B}$. In case that $\lambda = 1$, then $(X, \mathbb{B})$ is also known as a Steiner t-design, denoted by $S(t, v, k)$.

Definition 8.2.6. If $k < v$, a 2-(v, k, λ) design is called a balanced incomplete block design, BIBD in short. Notice that the term "balanced" comes from the fact that in a 2-(v, k, λ) design, for each $x \in X$, $r = r_x = \frac{\lambda(v-1)}{k-1}$ which is a constant. Another important fact is $bk = vr$. The following proposition is also clear to see.

Proposition 8.2.7. If $(X, \mathbb{B})$ is a 2-(v, k, λ) design, then $v > k$, $\frac{\lambda(v-1)}{k-1}$ and $\frac{\lambda v(v-1)}{k(k-1)}$ are integers.

Definition 8.2.8. An $(X, \mathbb{B})$ is called a pairwise balanced design (PBD in short), if any pair of elements in $\binom{X}{2}$, they occur together in exactly λ blocks of $\mathbb{B}$.

Notice that in a PBD, the blocks are not necessarily be of the same size. So, it is denoted by 2-(v, K, λ) design where $|X| = v$. and $K = \big\{|B| \,\big|B \in \mathbb{B}\big\}$.

Example 8.2.9. A 2-$(6, \{2, 5\}, 1)$ design.

$$X = \mathbb{Z}_6 \text{ and } \mathbb{B} = \big\{\{0, 1\}, \{0, 2\}, \{0.3\}, \{0.4\}, \{0, 5\}, \{1, 2, 3, 4, 5\}\big\}.$$

The following notions are not related to vector spaces.

An $(X, \mathbb{B})$ is *partial linear space*, if any two blocks of $\mathbb{B}$ contain at most one common element. If, indeed, any two elements (varieties) of a partial linear space occur together in a block of $\mathbb{B}$, then $(X, \mathbb{B})$ is a *linear space* with index 1. We may use "Geometry" to refer the above definitions:

1. Partial Linear Space : Any two lines intersect at most one point.

2. Linear Space : Any two points lie on a line (some line).

Now, we explore the relationship between $|X|$ and $|\mathbb{B}|$.

Theorem 8.2.10. (Fisher's inequality)
If $(X, \mathbb{B})$ is a 2-(v, k, λ) design, then $|X| \leq |\mathbb{B}|$.

Proof. Let A be the incidence matrix of $(X, \mathbb{B})$. Then $AA^T = (r-\lambda)I + \lambda J$, i.e., AA^T is a $v \times v$ matrix such that each entry in the diagonal is r and each entry outside diagonal is λ.

$$AA^T : \begin{array}{c} \\ x_1 \\ x_2 \\ \vdots \\ x_v \end{array} \begin{array}{c} \begin{array}{cccc} B_1 & B_2 & \cdots & B_b \end{array} \\ \left[\begin{array}{cccc} & & & \\ & & & \\ & & & \\ & & & \end{array}\right]_{v \times b} \end{array} \left[\begin{array}{ccc} & & \\ & & \\ & & \\ & & \end{array}\right]_{b \times v}$$

Observe that $AA^T(i, j)$ is the inner product of the i-th row and the j-th row. So, if $i = j$, it is the occurrence of x_i $\left(r_{x_i} = r\right)$ in the blocks of $\mathbb{B}$ and if $i \neq j$, it is the the number of blocks in which x_i and x_j occur together in the blocks, λ.

Now, we can find $\det(AA^T) = kr(r-\lambda)^{v-1}$. Since $AA^T = (r-\lambda)I + \lambda J$, an eigenvalue μ satisfies $(AA^T)\vec{x} = \mu\vec{x} = (r-\lambda)\vec{x} + \lambda J\vec{x} = (r-\lambda)\vec{x} + \lambda\mu'\vec{x}$ where μ' is an eigenvalue of J. By the fact that J is of rank 1, the set of eigenvalues of J are $\{v, \underbrace{0, 0, \cdots, 0}_{v-1}\}$.

Hence $\mu\vec{x} = \big((r-\lambda) + \lambda\mu'\big)\vec{x}$. This implies that $\mu = r - \lambda(v-1$ of them) and $\mu = r - \lambda + \lambda v = r + \lambda(v-1) = r + (k-1)r = kr$. Thus, $\det(AA^T) = kr(r-\lambda)^{v-1}$.

Since $v > k$, $\lambda < r$. This concludes that AA^T is non-singular, i.e., $\text{rank}(AA^T) = v$. Furthermore, $\text{rank}(AA^T) \leq \text{rank}(A) \leq \min\{v, b\}$, hence $b \geq v$. □

In fact, we have a stronger property on designs.

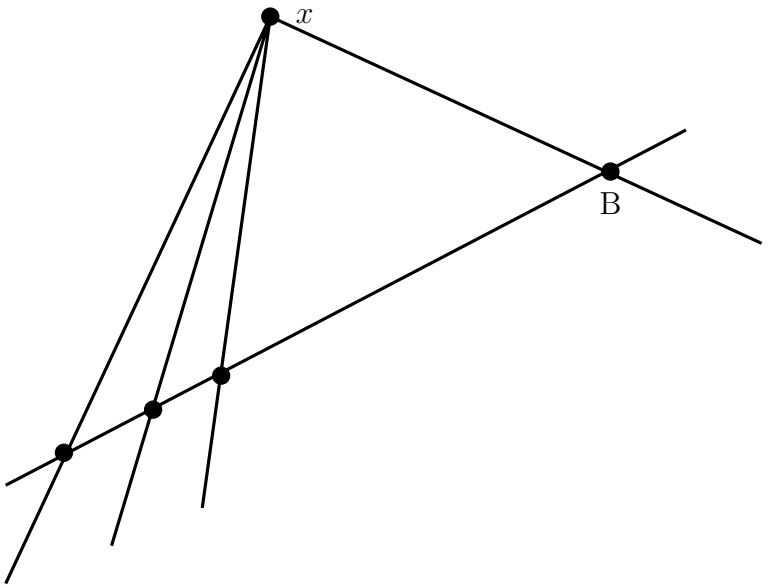
Theorem 8.2.11. If $(X, \mathbb{B})$ is a linear space, then $|X| \leq |\mathbb{B}|$.

Proof. Again, let $X = \{x_1, x_2, \cdots, x_v\}$ and $\mathbb{B} = \{B_1, B_2, \cdots, B_b\}$. Since $(X, \mathbb{B})$ is a linear space, any two elements in X occur together in a block of $\mathbb{B}$. Assume that $b \leq v$. If $x \notin B_i$, then $r_x \geq |B_i|$ since each element of B_i is going to occur together with x in some other blocks in $\mathbb{B}$. Now, we are ready for the following statement.

$$1 = \sum_{B \in \mathbb{B}} \frac{1}{b} = \sum_{B \in \mathbb{B}} \left(\sum_{x \notin B} \frac{1}{b(v - |B|)} \right) \tag{a}$$

$$1 = \sum_{x \in X} \frac{1}{v} = \sum_{x \in X} \left(\sum_{x \notin B} \frac{1}{v(b - r_x)} \right) \tag{b}$$

$$vr_x \geq b|B| \text{ for each } x \notin B. \ (v \geq b) \tag{c}$$



By (a),(b) and (c), $\sum_{B \in \mathbb{B}} \left(\sum_{x \notin B} \frac{1}{b(v-|B|)} \right) \leq \sum_{x \in X} \left(\sum_{x \notin B} \frac{1}{v(b-r_x)} \right)$
$\Rightarrow b \geq v$.
Hence, $b = v$. □

Remark 8.2.12. The equality $v = b$ also shows that $r_x = |B|$ for each $x \in X$ and $B \in \mathbb{B}$. The implication of this fact is that any two blocks intersect at exactly one element, i.e., $|B_i \cap B_j| = 1$, $1 \leq i \neq j \leq b$.

Definition 8.2.13. A BIBD is a square BIBD, denoted by SBIBD if $v = b$.

The following theorem is well-known, we state it and omit the proof here. (It is a "necessary condition" for the existence of an SBIBD).

Theorem 8.2.14. (Bruck-Ryser-Chowla,1949-1950)[3]
If a 2-(v, k, λ) design is a square BIBD, then

1. $k - \lambda$ is a square of an integer when v is even; and
2. $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}}\lambda y^2$ has a nonzero integral solution when v is odd.

8.3 Projective planes and Affine plances

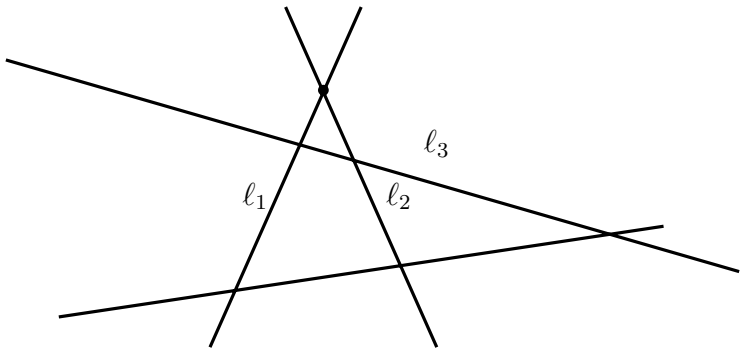
Definition 8.3.1. A projective geometry $\mathcal{P}$ is a (not necessarily finite) structure of points varieties and lines blocks such that

(P1) Every pair of points are on a unique common line;

(P2) Every line contains at least three points;

(P3) $\mathcal{P}$ containss a set of three points which are not on a common line;

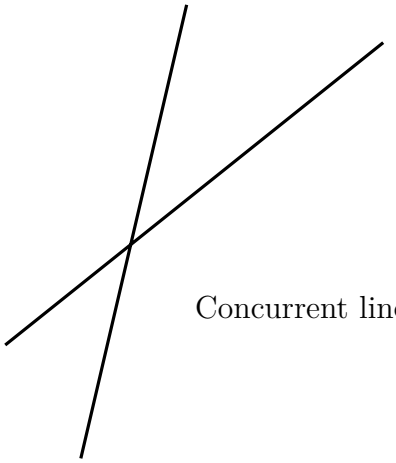
(P4) If a line intersects two sides of a triangle but not contain their common point then it intersects the 3rd side.



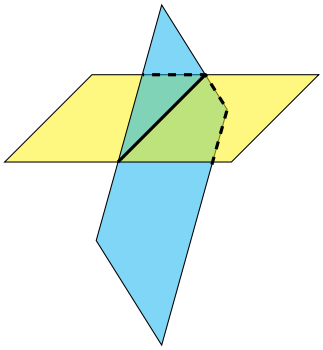
(P5) A projective plane is a projective geometry with this extra condition : every pair of distinct lines contain a common point.

Definition 8.3.2. Let V be an (n+1)-dim. vector space over $GF(q)$ where q is a prime power. The "projective geometry" $PG(n, q)$ is the geometry whose points, lines, planes, $\cdots$ are 1–, 2–, 3–, $\cdots$ dimensional subspace of V.

Definition 8.3.3. A (k+1)-dimensional subspace is called a k-flat, so that point is a o-flat, line is a 1-flat,$\cdots$, etc. All the flats are "varieties" in general term. Two varieties are "incident" if one contains the other, for example, a point on a line, a line on a plane, $\cdots$, etc. Two varieties are concurrent if their intersection is non-empty. (Say, two lines contain a common point.)



Concurrent lines



Concurrent planes

Proposition 8.3.4. The number of k-dim. subspace of an n-dim. vector space over $GF(q)$ is the Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q = \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$.

Observation 8.3.5.

(a) If we have a 2-dim. vector space V over $GF(q)$, then V contains q^2 vectors.

(b) There are $(q^n)(q^n - 1)(q^n - q) \cdots (q^n - q^{n-1})$ distinct bases in a vector space of dimension n.

(c) There are $(q^n - 1)(q^n - q) \cdots (q^n - q^{k-1})$ distinct bases in V which generate a k-dim. subspace.

Exercise. Prove proposition 8.3.4.

Proposition 8.3.6. Let V be a vector space of dimension n over $GF(q)$ and let U be an m-dim. subspace of V, $m \geq 0$. Then, the number of m+h-dim.

subspaces containing U is

$$\frac{(q^{n-m}-1)(q^{n-m}-q)\cdots(q^{n-m}-q^{h-1})}{(q^h-1)(q^h-q)\cdots(q^h-q^{h-1})}.$$

Proof. By the idea of counting bases we have the number:

$$\frac{(q^n-q^m)(q^n-q^{m+1})\cdots(q^n-q^{m+h-1})}{(q^{m+h}-q^m)(q^{m+h}-q^{m+1})\cdots(q^{m+h}-q^{m+h-1})}.$$

This implies the above result. □

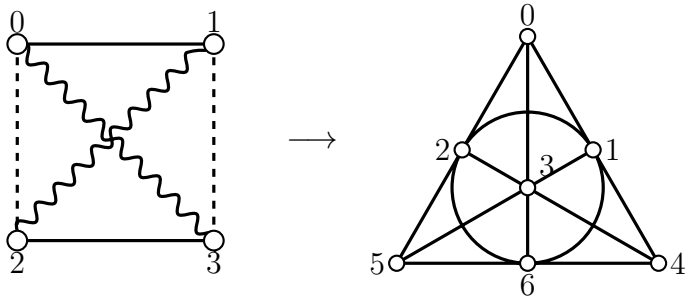
Definition 8.3.7. An Affine Geometry is obtained from a Projective Geometry by deleting a fixed hyperplane and all its subspaces.

Note that a Projective Geometry can also be obtained from an Affine Geometry.

Definition 8.3.8. A projective plane is a projective geometry $P(2,n)$ where n is a positive integer.

It is not difficult to see that a projective plane of order n is in fact a $2-(n^2+n+1,n+1,1)$ design and an affine plane is a $2-(n^2,n,1)$ design. For convenience, they are denoted by $PG(2,n)$ and $AG(2,n)$ respectively. Here are two examples.

Example 8.3.9.
$n=2$, $AG(2,2): X=\mathbb{Z}_4$, $\mathbb{B}=\Big\{\{0,1\},\{2,3\},\{1,2\},\{0,3\},\{1,3\},\{0,2\}\Big\}$



$AG(2,2)$ $PG(2,2)$

Example 8.3.10.
$n = 2$, $PG(2,2)$, $X = \mathbb{Z}_7$, $\mathbb{B} = \Big\{\{0,1,4\},\{2,3,4\},\{0,2,5\},\{1,3,5\},\{0,3,6\},$
$\{1,2,6\},\{4,5,6\}\Big\}$.

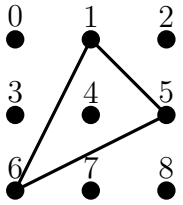
The projective plane of order 2 is also known as a Fano plane. By using a complete set of orthogonal latin squares of order n, we are above to prove that if n is a prime power, then both $PG(2,n)$ and $AG(2,n)$ exist. Instead of giving a proof, we use the following construction to explain the idea.

Orthogonal latin squares of order 3

$$\begin{array}{|c|c|c|}\hline 0&1&2\\\hline 1&2&0\\\hline 2&0&1\\\hline\end{array} \perp \begin{array}{|c|c|c|}\hline 0&1&2\\\hline 2&0&1\\\hline 1&2&0\\\hline\end{array} \Rightarrow \begin{bmatrix} 0&0&0&1&1&1&2&2&2\\ 0&1&2&0&1&2&0&1&2\\ 0&1&2&1&2&0&2&0&1\\ 0&1&2&2&0&1&1&2&0 \end{bmatrix}$$

$\Downarrow$

Affine plane of order 3



$\{1,5,6\} \in \mathbb{B}$

$\mathbb{B} = \Big\{\{0,1,2\},\{3,4,5\},\{6,7,8\},\{0,3,6\},\{1,4,7\},\{2,5,8\},\{0,4,8\},$
$\{1,5,6\},\{2,3,7\},\{0,5,7\},\{1,3,8\},\{2,4,6\}\Big\}$

$\Rightarrow$ Projective plane of order 3

By adding an infinite point to each parallel class, we have $PG(2,3) = (X,\mathbb{B})$, where $X = \{1,2,\ldots,8,\infty_1,\infty_2,\infty_3,\infty_4\}$ and $\mathbb{B} = \Big\{\infty_1,0,1,2\},$
$\{\infty_1,3,4,5\},\{\infty_1,6,7,8\},\{\infty_2,0,3,6\},\{\infty_2,1,4,7\},\{\infty_2,2,5,8\},$
$\{\infty_3,0,4,8\},\{\infty_3,1,5,6\}\{\infty_3,2,3,7\},\{\infty_1\infty_2,\infty_3,\infty_4\}\Big\}$.

Ex. Prove that for each prime power q, a $PG(2,q)$ and an $AG(2,q)$ exist.

8.4 Steiner systems

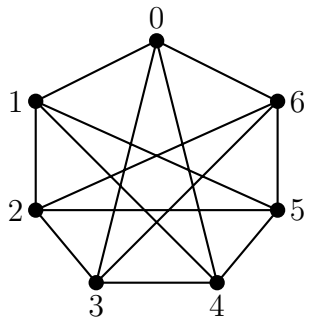
Definition 8.4.1. A $t-(v,k,\lambda)$ design is called a Steiner system if $\lambda = 1$.

Among all Steiner systems, Steiner triple system was studied around 170 years ago. In [7], R. T. Kirkman proved that a Steiner triple system of order v exists if and only if $v \equiv 1$ or 3 (mod 6). A Steiner triple system of order v, denoted by STS(v), is in fact a $2-(v,3,1)$ design. By $PG(2,2)$ and $AG(2,3)$, we know that a $2-(v,3,1)$ design exists when $v = 7$ and 9. Also, by the existence of such a design, we conclude that v has to be of the form $v = 6k+1$ or $v = 6k+3$ for each non-negative integer k. Therefore, it takes a great effort in constructing a $2-(v,3,1)$ design for $v \equiv 1$ or 3 (mod 6). So far, many different constructions are knows. Interesting readers may refer to [9] for more details. Here, we introduce one of them, which is known as a recursive construction.

Review that $\chi'(K_{2n}) = 2n-1$. Therefore, K_{2n} can be decomposed into $2n-1$ 1-factors $F_1, F_2, \cdots, F_{2n-1}$. Similarly, if G is a k-regular graph of even order and $chi'(G) = k$, then G can be decomposed into k 1-factors, say $G_1, G_2, \cdots, G_k$. The following notion is useful in modelling a network.

Definition 8.4.2. Let G be a graph defined on $\mathbb{Z}_v$. Let $D = \{d_1, d_2, \cdots, d_t\}$ where $d_i's$ are positive integers not greater than $\lfloor \frac{v}{2} \rfloor$. G is called a circulant graph with difference set D if two vertices i and j are adjacent whenever $|i-j|$ or $(v-|i-j|)$ are in D. For convenience, G is denoted by $G(v;D)$.

Example 8.4.3. $G(7;\{1,3\})$



It is easy to see that if v is odd, then $G(v;D)$ is a 2|D|-regular graph. If v is even, then the regularity may be odd provided $\frac{v}{2} \in D$. The graph $G(v;D)$ does have some great property. The following result is an excellent one. Since the proof is quite lengthy, we omit the details here.

Theorem 8.4.4. (Stern and Lenz, [11])

Let G be a circulant graph of even order v with $D = \{d_1, d_2, \cdots, d_t\}$. Then G is of Class 1, i.e., $\chi'(G) = \triangle(G)$ if $\frac{v}{2} \in D$.

Now, we are ready to construct all Steiner triple systems recursively.

Lemma 8.4.5. (v to $2v+1$ construction)

If there exists a STS(v), then there exists a STS($2v+1$).

Proof. Let X be a v-set and Y a (v+1)-set such that $X \cap Y = \emptyset$. Let $(X, \mathbb{B})$ be a STS(v) and $\{F_1, F_2, \cdots, F_v\}$ be a 1-factorization of K_{v+1} defined on Y. For convenience, we use $< x_i, F_i >$ to denote the set of triples $\{x_i, y_i', y_i''\}$ where $y_i'y_i''$ is an edge of F_i. Now, we obtain a collection of triples $\mathbb{B} = \mathbb{B}_1 \cup < x_i, F_i >_{i=1}^{v}$.

Since $\{F_1, F_2, \cdots, F_v\}$ is a 1-factor of K_Y, any two vertices y and y' of Y are going to be in a triple $< x_i, F_i >$ if $yy' \in F_i$. Similary, the two vertices between X and Y and inside X will be included in a triple of $\mathbb{B}$. Finally, $|\mathbb{B}| = \frac{v(v+1)}{6} + v \cdot \frac{v+1}{2} = \frac{(2v+1)(2v)}{6}$. This implies that $(X \cup Y, \mathbb{B})$ is indeed a STS($2v+1$). □

Lemma 8.4.6. (v to $2v+7$ construction)
If there exists a STS(v), then there exists a STS($2v+7$).

Proof. Since a STS(9) exists, it suffices to consider $v \geq 3$. By the existence of a STS(v), v is odd and thus $v+7$ is even and $v+7 \geq 10$. Let $X = \{x_1, x_2, \cdots, x_v\}$, $Y = \{y_1, y_2, \cdots, y_{v+7}\}$ and $(X, \mathbb{B}_1)$ be a STS(v). Now, consider the graphs G_1 and G_2 where $G_1 = \{y_i y_j |$the difference of i and j in $\mathbb{Z}_7$ is 1,2 or 3$\}$ and $G_2 = G(v+7; \{4, 5 \cdots, \frac{v+7}{2}\})$ defined on Y, i.e., G_2 is the complement of G_1 in K_Y. Since G_2 is a ciruclant graph $G(v+7; D)$ with $\frac{v+7}{2} \in D$, G_2 can be decomplosed into v 1-factors $F_1, F_2, \cdots, F_v$. On the other hand G_1 can be decomposed into $v+7$ triangles using the differences 1,2 and 3. Let the collection be $\mathbb{B}_2$.

Combining the above decomposition, we conclude that $(X \cup Y, \mathbb{B})$ is a STS($2v+7$) where $\mathbb{B} = \mathbb{B}_1 \cup \mathbb{B}_2 \cup < x_i, F_i >_{i=1}^{v}$. The details of checking can be obtained by a similar argument as Lemma 8.4.5. □

Theorem 8.4.7. A STS(v) exists if and only if $v \equiv 1$ or $3 \pmod 6$.

Proof. We prove the sufficiency here. The cases when v is 1 or 3 are trivial. Now, let $v \equiv 1$ or $3 \pmod 6$.
Case 1. $v = 12k+3$ and $v = 12k+7$.

By Lemma 8.4.5, They can be constructed by using a STS($6k+1$) and a STS($6k+3$) respectively.
Case 2. $v = 12k+1$ and $v = 12k+9$.

By Lemma 8.4.6, they can be constructed by using a STS($6k-3$) and a STS($6k+1$) respectively.

Hence for all $v \equiv 1$ or $3 \pmod 6$, there exists a STS(v). □

For block size larger than 3, the construction of Steiner systems is getting more complicate. The following result is known, but we skip the detail proof.

Theorem 8.4.8. [1] A $2-(v, 4, 1)$ design exists if and only if $v \equiv 1$ or $4 \pmod{12}$.

We can also consider t-designs for $t \geq 3$. The most popular 3-design is called a Steiner Quadruple System: a $3-(v, 4, 1)$ design (SQS(v)).

Lemma 8.4.9. If a $3-(v, 4, 1)$ design, SQS(v) exists, then $v \equiv 2$ or $4 \pmod 6$.

Proof. Let $(X, \mathbb{B})$ be a SQS(v). Let $x_0 \in X$ and $\mathbb{B}' = \{B \backslash \{x_0\} | x_0 \in B \text{ and } B \in \mathbb{B}\}$. Then, it is not difficult to check that $(X \backslash \{x_0\}, \mathbb{B}')$ is a STS($v-1$). Hence $v - 1 \equiv 1$ or $3 \pmod 6$. The proof follows. □

To show that for each $v \equiv 2$ or $4 \pmod 6$ a SQS(v) does exist is comparatively more complicate. H. Hanani[4] proved the sufficiency by using several recursive constructions. Later, a triple recursive construction was provided by A. Hartman [5]. So far, this construction remains the best. Here, we introduce a simpler case in construction.

Lemma 8.4.10. ($v \to 2v$ construction)
If a SQS(v) exists, then a SQS($2v$) exists.

Proof. Let $X = \{x_i | i \in \mathbb{Z}_v\}$ and $Y = \{y_i | i \in \mathbb{Z}_v\}$. Let $(X, \mathbb{B}_1)$ and $(Y, \mathbb{B}_2)$ be two SQS(v)'s respectively. Since v is even, K_X and K_Y can be decomposed into $v-1$ 1-factors respectively, say $\{F_1, F_2, \cdots, F_{v-1}\}$ and $\{F_1', F_2', \cdots, F_{v-1}'\}$. Now for $i = 1, 2, \cdots, v-1$, let $< F_i, F_i' >$ denote the collection of all 4-subsets $\{x_1, x_2, y_1, y_2\}$ such that x_1x_2 is an edge of F_1 and y_1y_2 is an edge of F_1'. By combining $\mathbb{B}_1$, $\mathbb{B}_2$, and all $< F_i, F_i' >$ for $i = 1, 2, \cdots, v-1$, we obtain a collection of 4-subsets $\mathbb{B}$.

Now, we claim that $(X \cup Y, \mathbb{B})$ is a $3-(2v, 4, 1)$ design, SQS($2v$). First, if a given 3-subset S of $X \cup Y$, $S \subseteq X$ or $S \subseteq Y$, then S is a subset of a 4-subset in $\mathbb{B}_1$ or $\mathbb{B}_2$ (respectively). So, consider $|S \cap X| \neq \emptyset$ and $|S \cap Y| \neq \emptyset$. Assume that $|S \cap X| = 2$, then those two elements will occur as an edge in some 1-factor F_i. Hence S will be a subset of a 4-subset in $< F_i, F_i' >$, since F_i' is also a 1-factor of K_Y. Similarly, for $|S \cap Y| = 2$ and $|S \cap X| = 1$, S is contained in a 4-subset of $< F_j, F_j' >$ provided the two elements in $S \cap Y$ are in an edge of F_j'.

So, it is left to check each 3-subset of $X \cup Y$ occurs exactly one in a 4-subset of $\mathbb{B}$. This follows from counting the size of $\mathbb{B}$. Since we need at least $\binom{2v}{3} / \binom{4}{3}$ 4-subsets to cover all distinct 3-subsets, i.e., at least $\frac{2v(2v-1)(2v-2)}{24}$ 4-subsets. By the fact, $|\mathbb{B}| = |\mathbb{B}_1| + \|\mathbb{B}_2\| + (v-1) \cdot (\frac{v}{2})^2 = 2 \cdot \frac{v(v-1)(v-2)}{24} + \frac{v^2(v-1)}{4} = \frac{2v(2v-1)(2v-2)}{24}$, we conclude the proof. □

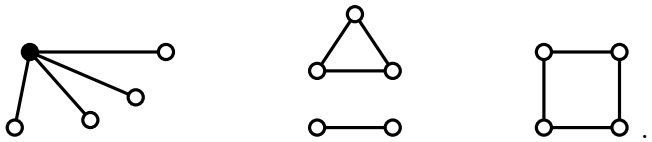
Notice that a $v \to 2v$ construction is not enough to construct all SQS(v) recursively. Unfortunately, we are not able to imitate the construction of STS(v) by giving a $v \to 2v + 6$ construction at this moment. It is believed that this construction probably is possible, but no one knows how to do it so far. If indeed we have this construction, then all SQS(v)'s can be constructed

recursively with ease.

We shall close this section with the statement of the above "desired" construction.

Problem Can we construct a SQS($2v + 6$) which contains a subsystem of order v?

Exercise 1. Let X be the set of edges in a complete graph of order 5, K_5. Prove that a SQS(10) can be obtained by using the following subgraphs of K_5:



Exercise 2. Let $X = (\mathbb{Z}_2)^n$ and $\mathbb{B} = \left\{\{\vec{x}, \vec{y}, \vec{z}, \vec{w}\} \mid \vec{x}, \vec{y}, \vec{z}, \vec{w} \in (\mathbb{Z}_2)^n \text{ and } \vec{x} + \vec{y} + \vec{z} + \vec{w} = \vec{0}\right\}$. Show that $(X, \mathbb{B})$ is a SQS(2^n).

Exercise 3. Let $X = \mathbb{Z}_8$. Show that there exist a SQS(8) defined on X such that $\{0, 1, 2, 3\}$ intersects all the blocks of this SQS(8).

References

[1] A. E. Brouwer, Some nonisomorphic BIBD $(4, 1, v)$, Math. Centrum Amsterdam, ZW102(1977).

[2] R. C. Bose, E. T. Parker and S. Shrikhande, On the construction of sets of mutually orthogonal latin squares and the falsity of a conjecture of Euler, Trans. Amer. Math. Soc. 95(1960), 191-209.

[3] R. H. Bruck and H. J. Ryser, The nonexistence of certain finite projective planes, Can. J. Math. 1(1949),88-93.

[4] H. Hanani, On quadruple systems, Canad. J. Math. 12(1960), 145-157.

[5] A. Hartman, A general recursion construction for quadruple systems, J. Combin. Th. (A), 33(1982), 121-134.

[6] Jacques Ozanam, Court cards problem, Recreation mathematiques et physiques(1725), Vol.IV, p.434.

[7] R. T. Kirkman, On a problem in combinations, Camb. and Dublin Math. J. 2(1847), 191-204.

[8] Leonhard Euler, Recherches sur une nouvelle especе de quarres magiques, 1779.

[9] C. C. Lindner and C. A. Rodgerr, Design Theory, CRC Press, Boca Raton, New York(1997).

[10] P. Hall, On representatives of subsets, J. London Math. Soc. 10(1935), 26-30.

[11] G. Stern and H. Lenz, Steiner triple systems with given subspaces; another proof of Doyen-Wilson theorem, Boll. Un. Mat. Ital. (5). 17-A(1980), 109-114.