Lectures on Combinatorial Designs

Contents

1 Introduction of Combinatorial Design

Let $\mathbb{X}$ be a finite non-empty set. A collection of subsets of $\mathbb{X}$, $\mathbb{B}$ contains at most $2^{\mathbb{X}}$. For distinct subsets, there are exactly $\binom{v}{k}$ k-subsets if $|\mathbb{X}| = v$.

(·) $\sum_{k=0}^{v} \binom{v}{k} = 2^v$

This is a direct consequence of $(1+x)^v = \sum_{k=0}^{v} \binom{v}{k} x^k$.

For convenience, we shall use $\mathbb{Z}_v = \{0, 1, 2, \cdots, v-1\}$ for $\mathbb{X}$.

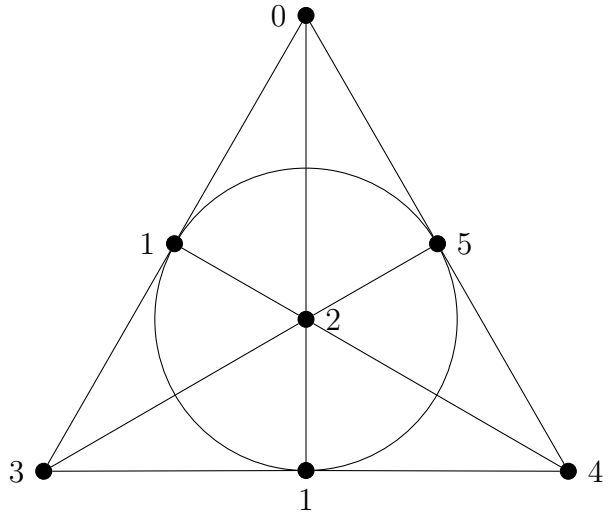
The reason comes from the fact that $< \mathbb{Z}_v, +, \cdot >$ is a commutative ring. So, we can apply the operation if necessary. For example, $\{0,1,3\}$ is a 3-subset of $\mathbb{Z}_7$. $\{0,1,3\}+1 := \{0+1, 1+1, 3+1\} = \{1,2,4\}$ is also a 3-subset of $\mathbb{Z}_7$, then $\{0,1,3\} \cdot 2 := \{0 \cdot 2, 1 \cdot 2, 3 \cdot 2\} = \{0,2,6\}$ is a 3-subset of $\mathbb{Z}_7$ as well.

(⋆) We are learning the construction of $(\mathbb{X}, \mathbb{B})$ which satisfies extra conditions! For examples,

1. No subset of $\mathbb{B}$ is contained in the other subset of $\mathbb{B}$.
2. No two subsets of $\mathbb{B}$ have an empty intersection.
3. Any two elements of $\mathbb{X}$ occur together in a subset of $\mathbb{B}$ exactly once.
4. The union of any d subsets of $\mathbb{B}$ are all distinct for $d \geq 2$.
5. Each t-subset of $\mathbb{X}$ occurs exactly λ times in subsets of $\mathbb{B}$.

(·) **Extremal sets corresponding to above examples**

1. If $|\mathbb{X}| = n$, then we can choose all subsets of cardinality $\left\lfloor \frac{n}{2} \right\rfloor + 1$. This implies that $|\mathbb{B}| \geq \binom{n}{\left\lfloor \frac{n}{2} \right\rfloor + 1}$.
2. Let $x_0 \in \mathbb{X}$. Then, all subsets of $\mathbb{X}$ containing x_0 provides a collection. This implies that $|\mathbb{B}| \geq 2^{n-1}$.
3. For example. If $|\mathbb{X}| = 7$, let $\mathbb{X} = \mathbb{Z}_7$ and $\mathbb{B} = \{\{0,1,3\} + i \mid i \in \mathbb{Z}_7\}$. This is the well-known Fano plane.



Fano plane

Fact 1. A design $(\mathbb{X}, \mathbb{B})$ can be treated as a hypergraph defined on the vertex set $\mathbb{X}$, and $B \in \mathbb{B}$ is an edge (hyperedge).

Fact 2. We can define $G_{\mathbb{X},\mathbb{B}}$ (a bipartite graph with partite sets $(\mathbb{X}, \mathbb{B})$) such that $x_i \sim B_j$ if and only if $x_i \in B_j \subseteq \mathbb{X}$ and $B_j \in \mathbb{B}$. Then, its incidence matrix $A(G_{\mathbb{X},\mathbb{B}})$ is as follows.

$$A_{i,j} = \begin{cases} 1, & x_i \in B_j \\ 0, & \text{otherwise} \end{cases} \qquad A\left(G_{\mathbb{X},\mathbb{B}}\right) = \begin{array}{c} \\ x_1 \\ \vdots \\ x_i \\ \vdots \\ x_v \end{array} \begin{array}{c} \begin{array}{cccccc} B_1 & \cdots & B_j & \cdots & B_b \end{array} \\ \begin{bmatrix} & & \vdots & & \\ & & \vdots & & \\ \cdots & \cdots & 1 & & \\ & & & & \\ & & & & \end{bmatrix} \end{array}$$

Fact 3. Since $G_{\mathbb{X},\mathbb{B}}$ can be represented by a $v \times b$ $(0,1)$-matrix, a design $(\mathbb{X}, \mathbb{B})$ can be viewed as a $(0,1)$-matrix.

Fact 4. A design $(\mathbb{X}, \mathbb{B})$ can be represented by b (binary) codewords which are the columns of $A\left(G_{\mathbb{X},\mathbb{B}}\right)$. Let $\mathbf{a}$ be a binary (column) vector of length v. Hence, a design can be considered as a set of codewords of length v where $|\mathbb{X}| = v$.

($\cdot$) An n-dimension $(0,1)$-vector is called a (binary) codeword of length n.

($\cdot$) A binary code of length n is a collection of codewords of length n.

($\cdot$) A "codeword" can be utilized to represent a

(i) message

(ii) signal

(iii) transmitting scheme

(iv) data pattern

(v) many others

e.g. (1,1,0,1,0,0,0) is a "codeword" of length 7.

Definition 1.1.

Let $\mathbf{a} = (a_0, a_1, \cdots, a_{n-1})$ be a (0,1)-vector. Then, the support of $\mathbf{a}$, $supp(\mathbf{a}) = \{i | a_i = 1, i = 0, 1, 2, \cdots, n-1\}$. Clearly, $supp(\mathbf{a}) \subseteq \mathbb{Z}_n$.

($\star$) If there are exactly k one's in $\mathbf{a}$, than $supp(\mathbf{a})$ is a k-subset of $\mathbb{Z}_n$.

Designs $\Longleftrightarrow$ Codes

($\star\star$) There are beautiful designs which are obtained from the construction of codes. On the other hand, (good) codes can be obtained by using designs.

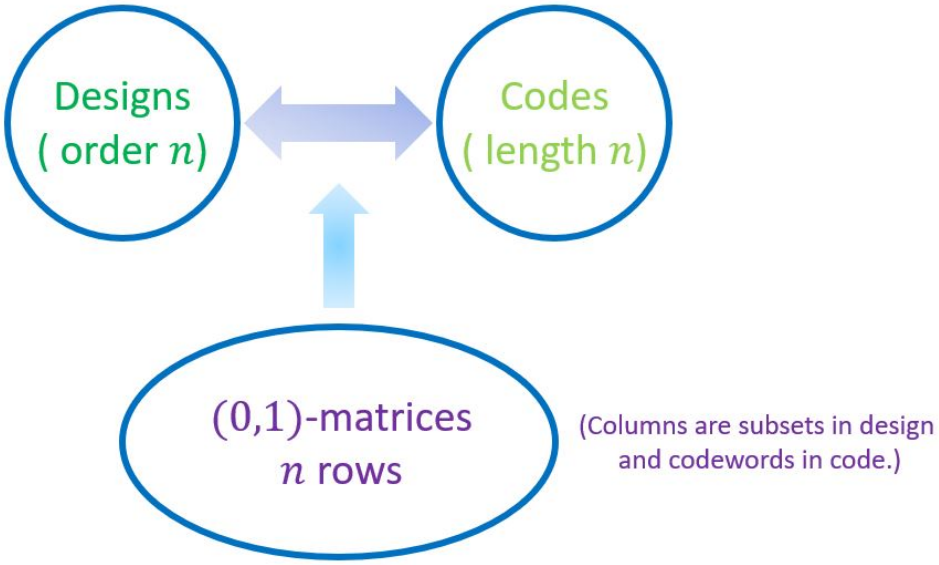


Figure 1: Designs and codes

(·) We can extend the binary code to the q-ary code in which $\{0,\}$ is replaced by $\{0,1,2,\cdots,q-1\}$. But, binary code is still more "important"!

(·) There are deterministic and probabilistic methods to construct designs (codes), $(0,1)$-matrices as well.

2 Latin Square

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

In fact, the eariliest reference to the use of such squares can be dated back to 18 Century. At that time, people are placing the sixteen court cards (A, K, Q, J) of a pack of ordinary playing cards in the form of a square so that no row, column, or diagonal should contain more than one card of each suit and one card of each rank. The solution was obtained in **1723**. Here is an example.

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

$S \to 1,\ H \to 2,\ D \to 3,\ C \to 4$

But, the real impact comes from the famous **36 officers problem** proposed by Euler around 10 years later. So, 16 cards are extended to 36 cards. Unfortunately, this plan turns out to be impossible. The proof by "brute force" was obtained around 1900 by

Tarry. A theoretical argument to show that it is not possible came out after around 80 years by D.R. Stinson (1984).

Nowadays, the applications of using Latin Squares have been everywhere. It is a topic worth of study.

Definition 2.1. (Latin Square of order n)

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

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

Quasigroup

1st 2nd 3rd

↓ ↓ ↓

1st →

2nd →

3rd →

0	1	2
1	2	0
2	0	1

Latin Square of order 3

Remark. We can use any n-set for S, say $S = \{\alpha, \beta, \gamma\}$.

α	β	γ
β	γ	α
γ	α	β

a Latin square of order 3

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

Fact 1 A Latin square of order n exists for each $n \in \mathbb{N}$.

Fact 2 A Latin square of order n can be obtained from the fact $\chi'(K_{n,n}) = n$. (Edge coloring of $K_{n,n}$)

Fact 3 The existence of a Latin square of order n is equivalent to the existence of $K_3 | K_{n,n,n}$. (Graph decomposition)

Fact 4 Let ℓ_n denoted the number of distinct Latin squences of order n. Then $\ell_1 = 1,\ \ell_2 = 2,\ \ell_3 = 12,\ \ell_4 = 576,\ \ell_5 = 161,280,\ \cdots$. ($L \neq L'$ if and only if $L_{i,j} \neq L'_{i,j}$ for some (i,j))

Fact 5 $\ell_9 = 9!\,8!\,(377,597,964,258,816)$.
Check Wiki for more imformation.

Fact 6 A Latin square of order n can be obtained from the operation table of a "**quasigroup**" of order n.

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

$S = \{0, 1, 2\},\ \langle S, * \rangle$ is a quasigroup of order 3.

3!
↓

0	1	2	3	← 4!
1				
2				
3				

By using permutations of 0, 1, 2, 3, we can obtain a Latin square of "standard form". (above)

0	1	2	3
1	(0)		
2		(0)	
3			

0	1	2	3
1	(0)		
2		(1)	
3			

0	1	2	3
1	(2)		
2			
3			

0	1	2	3
1	(3)		
2			
3			

Now, there are 4 ways to finish filling all the other entries by choosing "**typical**" entries first. (Similar to Sudoku)

$\ell_4 = 4 \times 4! \times 3!$

$\ell_5 = \boxed{?} \times 5! \times 4!$

$\boxed{?} = 56$

Algebraic Structure (Basic ideas)

Single speration

Definition 2.2. (Binary operation)

A binary operation (defined on) A is a mapping $\circ : A \times A \to A$.

For convenience $\circ((a,b)) = c$ is denoted by $a \circ b = c$.

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

Definition 2.3. (Algebraic Struture in one operation)

An ordered pair $\langle A, \circ \rangle$ is a **groupoid** if "$\circ$" is a binary operation defined on A.

Besides binary operation, an operation may satisfy more "laws".

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

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

(3) Identity : e is an identity of $\langle A, \circ \rangle$ if $\forall \alpha \in A,\ \alpha \circ e = e \circ \alpha = \alpha$.

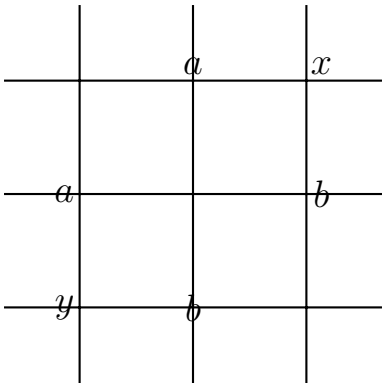
(4) Inverse: a is an inverse of b (in A) if $a \circ b = b \circ a = e$.

(3)′ Right Identity : $a \circ e = a$
Left Identity : $e \circ a = a$

(4)′ Right Inverse : $a \circ b = e$
Left Inverse : $b \circ a = e$

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

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



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

Definition 2.4. (Quasigroup)

If $\langle A, \circ \rangle$ satisfies row and column Latin-property, then $< A, \circ >$ is a quasigroup. If A is a finite set, then its operation table corresponds to a Latin square of order $|A|$.

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

1. (0) + (1) $\longrightarrow$ Semigroup

2. ⓪ + ① + ③ ⟶ Monoid

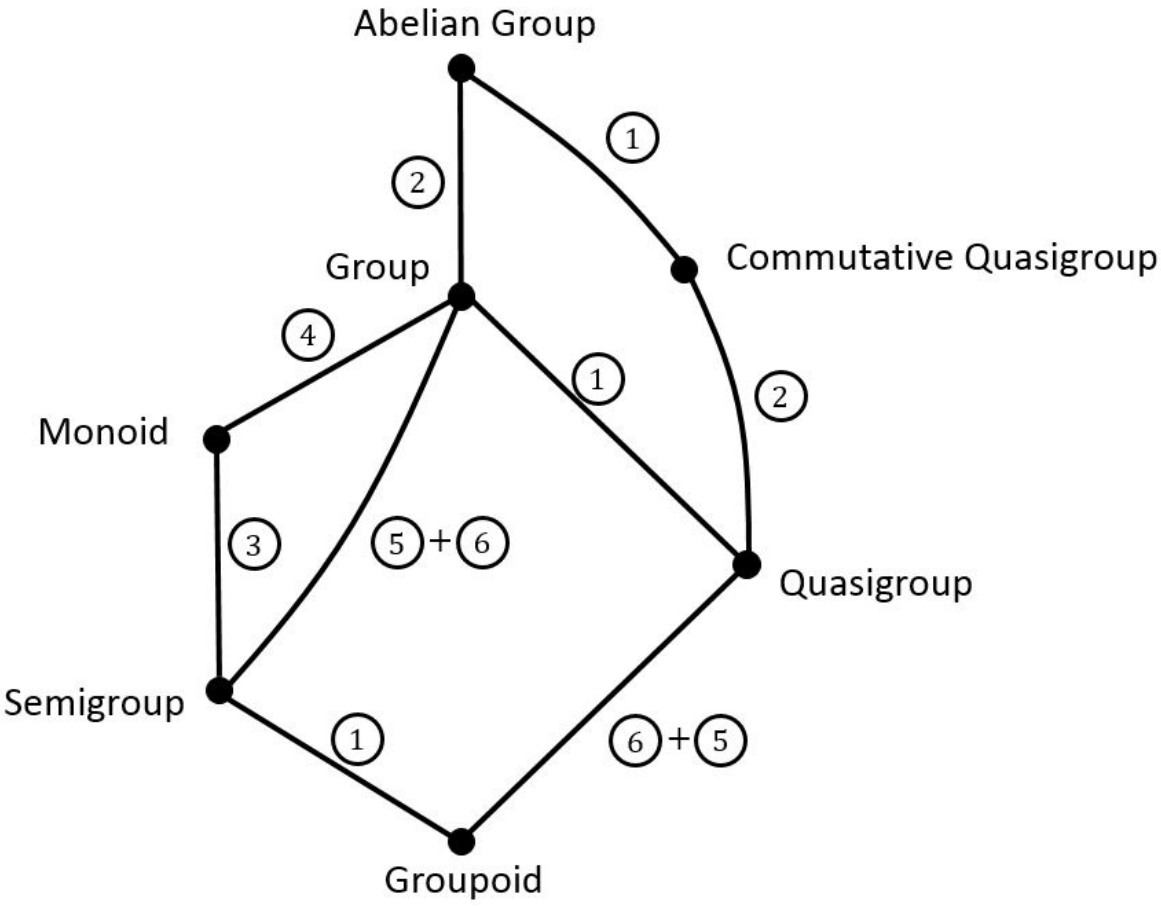
3. ⓪ + ① + ③ + ④ ⟶ Group

4. ⓪ + ① + ② + ③ + ④ ⟶ Abelien Group

5. ⓪ + ⑤ + ⑥ ⟶ Quasigroup

6. ⓪ + ① + ⑤ + ⑥ ⟶ Group

7. ⓪ + ② + ⑤ + ⑥ ⟶ Commutative Quasigroup



Fact 7 We shall adapt the property of a quasigroup of order n to "**claim**" the property of its corresponding Latin square.

e.g. If $\langle Q, * \rangle$ is a commutative quasigroup of order n, then its corresponding Latin square is a **commutative** Latin square or sometime a "**symmetric**" Latin square.

Definition 2.5. (Idempotent and Unipotent)

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

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

Idenpotent and Commutative L.S.
$\approx\ \chi'(K_n) = n$. (n is odd)

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

Unipotent and Commutative L.S.
$\approx\ \chi'(K_n) = n - 1$. (n is even)

The construction of idempotent commutative Latin Square

For each odd n, we define an abelian group $\langle \mathbb{Z}_n, + \rangle$. For example, $n = 7$.

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

$\Uparrow$

A diagonal commutative L.S.

$$\Downarrow$$

use permutation

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 \end{pmatrix}$$

$$\Downarrow$$

An idempotent commutative L.S.

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

$$\Downarrow$$

A Unipotent commutative L.S. of order 8

Fact 8 Permuting rows, columns or entries of a Latin square provide another Latin square.

Fact 9 (Latin square of standard form)
There exists a Latin square of order n (based on $\mathbb{Z}_n$), such that its first row is $(0, 1, 2, \cdots, n-1)$ and its first column is $(0, 1, 2, \cdots, n-1)$.

$(*)$ There are exactly "4" Latin squares of order 4 which are of standard form. $\ell_4 = 4! \cdot 3! \cdot 4 = 576$. $\ell_5 = 5! \cdot 4! \cdot 56 = 161,280$.
$(*)$ (56) for order 5 and (9408) for order 6.

0	1	2	3
1	(0)	3	2
2	3	$\begin{smallmatrix}0\\1\end{smallmatrix}$	$\begin{smallmatrix}1\\0\end{smallmatrix}$
3	2	$\begin{smallmatrix}1\\0\end{smallmatrix}$	$\begin{smallmatrix}0\\1\end{smallmatrix}$

↑
Two choice

0	1	2	3
1	(2)	3	0
2	3	0	1
3	0	1	2

One choice

0	1	2	3
1	(3)	0	2
2	0	3	1
3	2	1	0

One choice

(∗∗) Basically, this is the idea of counting distinct Latin squares.

Fact 10 Let $\langle Q, \circ \rangle$ be a quasigroup. Define $\langle Q, \circ \rangle$ where $a * c = b$ provided $a * b = c$ for all $a, b, c \in Q$.

Then, $\langle Q, \circ \rangle$ is also a quasigroup. (Conjugate)

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

$0 \circ 0 = 0$
$0 \circ 1 = 1$
$0 \circ 2 = 2$
$1 \circ 0 = 1$
$1 \circ 1 = 2$
$1 \circ 2 = 0$
$2 \circ 0 = 2$
$2 \circ 1 = 0$
$2 \circ 2 = 1$
↑ ↑ ↑
a b c

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

$0 * 0 = 0$
$0 * 1 = 1$
$0 * 2 = 2$
$1 * 1 = 0$
$1 * 2 = 1$
$1 * 0 = 2$
$2 * 2 = 0$
$2 * 0 = 1$
$2 * 1 = 2$
↑ ↑ ↑
a c b

$a \circ b = 0$ (Six conjugate quasigroups!)

$\Downarrow$

$a * c = b\ ,\ b *' c = a\ ,\ c *'' a = b\ ,\ c *''' b = a\ ,\ b *'''' a = c\ .$

$\downarrow$ (check)

$\begin{pmatrix} \forall\ \alpha, \beta,\ \alpha *'' x = \beta \text{ has a unique solution } \gamma \text{ since } \gamma \circ \beta = \alpha. \\ \text{Similarly, } y *'' \alpha = \beta \text{ has a solution } \gamma' \text{ if } \alpha \circ \beta = \gamma'. \end{pmatrix}$

They are called **conjugate quasigroups** and therefore we have conjugate Latin squares of order 3.

Isotopic Classes

Definition 2.6. (Isotopism)

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

Check :

If $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$ are **isotopic**, then we say there exists are isotopism between $\langle Q_1, \circ \rangle$ and $\langle Q_2, * \rangle$. Prove that "isotopism" is an equivalence relation.

Remark. Since isotopism is an equivalence relation, we can partition the set of distinct Latin squaresof order n in to isotopic classes.
For example, there are two isotopic classes of order 5 and 22 isotopic classes for order 6. (Only one isotopic class for order 1, 2 and 3; two classes for order 4.)

3 Partial Latin Squares

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

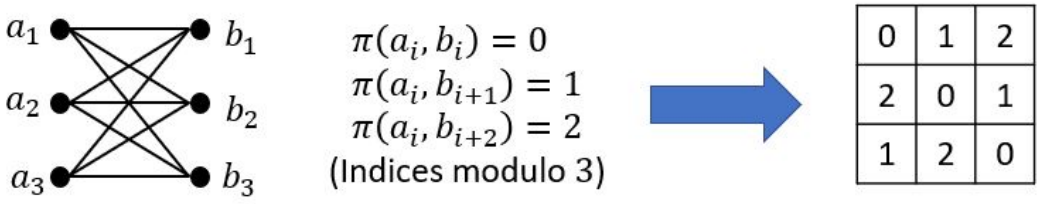
Let $G = (V, E)$ be a graph. A k-edge-coloring π of G is a mapping $\pi : E \to \{1, 2, \cdots, k\}$ such that $\pi(e) \neq \pi(f)$ provided e and f are incident edges in G. The minimum integer k such that G has a k-edge-coloring is called the chromatic index of G, denoted by $\chi'(G)$. The following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

Fact 1. If G is a simple graph, then $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.

Fact 2. If G is a bipartite graph, then $\chi'(G) = \Delta(G)$.

Fact 3. The edge-coloring $\chi'(K_{n,n})$ corresponds to a Latin square of order n.

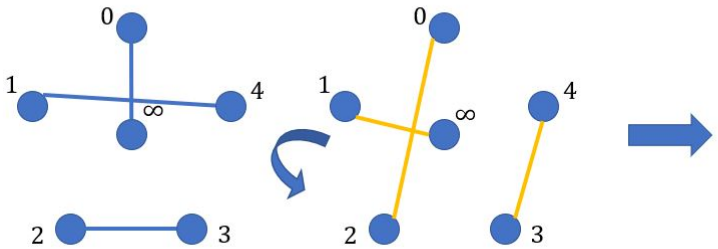
($\star$) The number of distinct n-edges-colorings of $K_{n,n}$ gives l_n.



($\star$) A unipotent Latin square of order n can be constructed accordingly.

($\star$) We can use $\chi'(K_{2m+1}) = 2m + 1$ to construct an idempotent commutative Latin square.

Example $m = 2$



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

($\star$) There does not exist an idempotent commutative Latin square of even order.

Sub-squares

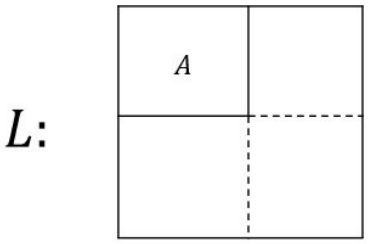
Just like algebraic structures, we have sub-quasigroup, and those subsquares.

Definition 3.1. (sub-Latin square)

If $Q' \subseteq Q$, $< Q', \circ >$ and $< Q, \circ >$ are quasigroups, then $< Q', \circ >$ is called a sub-quasigroup of $< Q, \circ >$. Their corresponding Latin squares are Latin square and Latin subsquare respectively.

Definition 3.2. (Embedding)

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



Theorem 3.3.

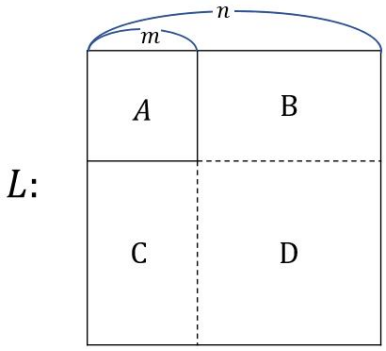
A latin sbsquare of order m can be embedded in a Latin square of order n if and only if $n \geq 2m$.

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

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

Proposition 3.4. If A is embedded in L and $L(i)$ denotes the number of element i occurs in L (respectively A, B, C, D in next figure), then $A(i) \geq 2m - n$ where A is a Latin square of order m and L is a Latin square of order n.

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

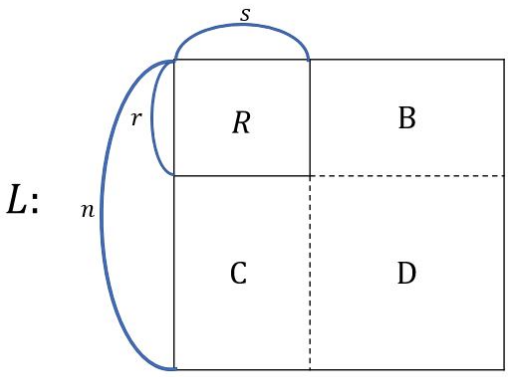


Corollary 3.5. (The sufficient condition of Theorem 3.3 is true)

If a Latin subsquare of order m can be embedded in a Latin square of order n, then $n \geq 2m$.

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

In fact, the subsquare A we consider here can be replaced by Latin rectangle or partial Latin rectangle. Let R be a partial Latin rectangle of L.



R is embedded in a Latin square L

Proposition 3.6.

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

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

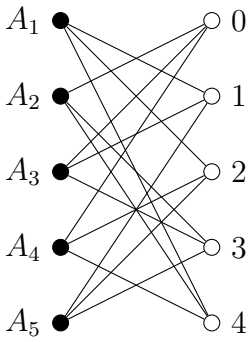
Proposition 3.7.

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

Proof. SDR (system of distinct representatives) or $K\ddot{o}nig's$ Theorem. □

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

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



Fact 3. Let R be an $r \times s$ partial Latin rectangle. Then R can be embedded in a Latin square of order n based on S if and only if $R(i) \geq r + s - n,\ \forall i \in S\ (|S| = n)$.

Proof. (Outline)

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

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

Step 3. Complete the Latin square by extending the rectangle. The details are obtained by using two theorem.

Theorem 3.8. (P. Hall, 1935)

$\{S_1, S_2, \cdots, S_n\}$ has an SDR if and only if the union of any k of them contains at least k elements.

Proof. ($\Rightarrow$) Trivial.

($\Leftarrow$) By induction on n and it's clearly true for $n = 1$. Assume that the assertion is true for all $1 \leq m < n$ and consider $\{S_1, S_2, \cdots, S_n\}$.

Case 1. $\forall k \leq n - 1, |\cup_{j=1}^{k} S_{i_j}| \geq k + 1$.

Let $x_n \in S_n$ and consider $\{S_1 \setminus \{x_n\}, S_2 \setminus \{x_n\}, \cdots, S_{n-1} \setminus \{x_n\}\}$. By induction, this collection of sets does satisfy the Hall's condition, it has an SDR $x_1, x_2, \cdots, x_{n-1}$. Together with x_n, we have the proof.

Case 2. $\exists h \leq n - 1, |\cup_{j=1}^{h} S_{i_j}| = h$.

Let $\cup_{j=1}^{h} S_{i_j} = \tilde{S}$. For convenience, let those h subsets be $S_1, S_2, \cdots, S_h$. Now, consider $S_{h+1} \setminus \tilde{S}, S_{h+2} \setminus \tilde{S}, \cdots, S_n \setminus \tilde{S}$. The union of any k of these sets must contain at least k elements. For otherwise, the union of $\tilde{S}$ with these sets will contain less than $h + k$ elements, a contradiction to the assumption. Hence, $\{S_{h+1} \setminus \tilde{S}, S_{h+2} \setminus \tilde{S}, \cdots, S_n \setminus \tilde{S}\}$ has an SDR. Also, $\{S_1, S_2, \cdots, S_h\}$ has an SDR. Together, we have an SDR for $\{S_1, S_2, \cdots, S_n\}$. □

Theorem 3.9. (A. J. Hoffman and H. W. Kuhn, 1956)

Let M be a given set. A necessary and sufficient condition for the sets $S_1, S_2, \cdots, S_n$ to have an SDR which includes all the element of M is that, for every $M' \subseteq M$, at least $|M'|$ of the sets $S_1, S_2, \cdots, S_n$ have non-empty intersection with M'. (Note that $\{S_1, S_2, \cdots, S_n\}$ has an SDR itself.)

Since the proof of Theorem **??** needs more effort, we omit the proof here. But, we shall apply this result to prove the embedding theorem mentioned above.

Definition 3.10. (Partial Latin Square of order n) PLS(n)

A PLS(n) is an $n \times n$ array such that each cell is either filled with an entry from an n-set S or empty, moreover, each element in S occurs at most once in each row and resp. once in each column.

Definition 3.11. (Complete the PLS(n))

Let L' be a PLS(n). L' is said to be completable if we can fill all the empty cells such that the $n \times n$ array is a Latin square.

0	1	
		2

incompletable

0	1	
1		

completable

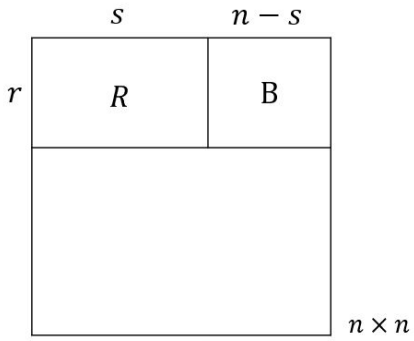
Theorem 3.12. (H. J. Ryser, 1951)

Let R be an $r \times s$ Latin rectangle based on $S = \{1, 2, \cdots, n\}$ (filled partial Latin square). Then, R can be embedded in a Latin square of order n if and only if $R(i) \geq r + s - n$ for all $i \in S$.

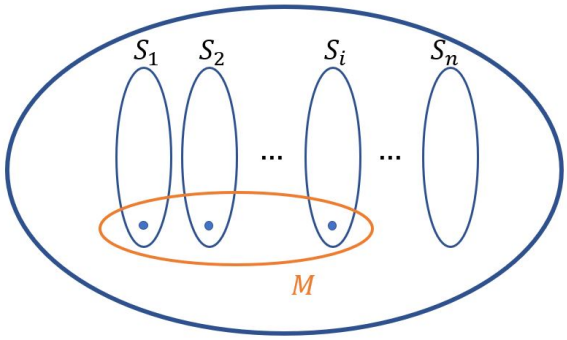
Proof. The proof of necessity has been done earlier, we prove the sufficiency in what follows. We claim that R can be enlarged to an $r \times (r+1)$ rectangle R^* such that $R^*(i) \geq r + (s+1) - n, \forall i$. Iteration then extends R to an $r \times n$ rectangle. Then, we obtain a Latin square of order n by applying M. Hall's extension theorem.

Let S_j denote the set of elements in S which do not occur in the jth row of R. Now, let M be the set of elements in R occurred **exactly** $r+s-n$ **times**. The proof follows by showing $\{S_1, S_2, \cdots, S_r\}$ has an SDR such that the set of elements in S still satisfy the necessary condition. Now, we claim that $|M| \leq r$.

If there are more elementss which occur exactly $r+s-n$ times, say $r+r', r' > 0$, then other $n-(r+r')$ elements will occur at most r times. Hence, in total we have $(r+r')(r+s-n) + (n-r-r') = r^2 + rs + rr' + r's - rn - r'n + nr - r^2 - rr' = rs + r's - nr' = rs - r'(n-s) < rs$ entries for R, $\rightarrow\leftarrow$.



Now, since $M = \{i | R(i) = r+s-n, i \in \mathbb{Z}_n\}$, $\forall x \in M$, x occurs in $S_1 \cup S_2 \cup \cdots \cup S_r$ exactly $r-(r+s-n) = n-s$ times. Moreover, for the other $y \in \mathbb{Z}_n \setminus M$, y occurs in the union at most $n-s$ times. As a consequence, elements from M are in total $|M| \cdot (n-s)$ entries in $S_1 \cup S_2 \cup \cdots \cup S_r$. Since $|S_i| = n-s$ for $i = 1, 2, \cdots, r$, at least $|M|$ of sets in $\{S_1, S_2, \cdots, S_r\}$ have non-empty intersection with M. This is also true for $M' \subseteq M$.



So, by Hoffman and Kuhn Theorem, there exists an SDR of $S_1, S_2, \cdots, S_r$ such that all elements of M are included in the SDR. This implies that R can be extended to an $r \times (s+1)$ partial Latin square (rectangle), $\tilde{R}$, such that $\forall x \in \mathbb{Z}_n$, $\tilde{R}(x) \geq r + (s+1) - n$. This can be done until $s = n - 1$. Therefore, we obtain an $r \times n$ Latin rectangle. By using theorem 1 (Hall's Theorem), we can embed R into a Latin square of order n. $\square$

4 Critical Sets

$(*)$ It is interesting to know whether a PLS(n) can be completed to a Latin square.

Fact 1 A PLS(n) with at most $n-1$ filled cells can be completed to a Latin square of order n. (Evan's Conjecture)

(In fact, the proof of this fact is not very difficult.) Proved by B. Smetaniuk (1981). You may refer to " A course in combinatorics " by J.H van Lint and R.M. Wilson, page 189-193.

Fact 2 It takes about 50 pages to characterize a PLS(n) with at most $n+1$ filled cells which is completable.

(L.D. Anderson and A.J.W. Hilton, 1983, LMS.)

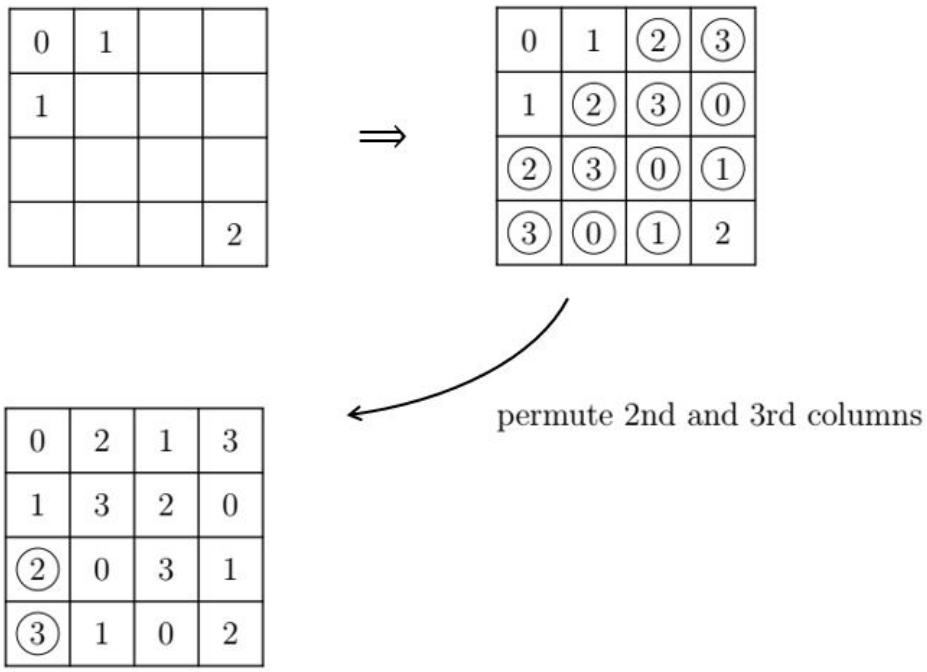
$(\cdot)$ n filled cells may be too much!

0	1	2	
			3

0			
	0		
		0	
			1

Definition 4.1. (Critical Sets)

A partial Latin square C is called a **crtical set** of a Latin square L if (a) the empty cells of C can be filled to obtain L and (b) any proper sub-partial square of C can be completed to at least two distinct Latin squares (one of them is L).



(∗) A critical set of order n contains at least $n-1$ distinct elements and covers at least $n-1$ rows, resp. $n-1$ columns.

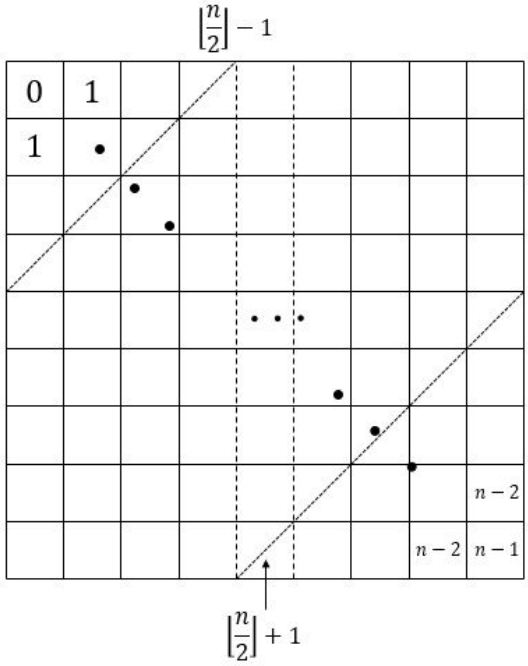
(•) Sudoku is a special critical set of order 9.

Fact We can construct a (strong) critical set C of order n with $|C| = \lfloor \frac{n^2}{4} \rfloor$.

(0)	2	1
2	1	0
1	0	(2)

(0)	(1)	3	2
(1)	3	2	0
3	2	0	1
2	0	1	(3)

(0)	(1)	3	4	2
(1)	3	4	2	0
3	4	2	0	1
4	2	0	1	(3)
2	0	1	(3)	(4)



Problem If C is a crtical set of order n, then find $\min|C|$ and $\max|C|$.

Conjecture $|C| \geq \lfloor \frac{n^2}{4} \rfloor$.

Construction of Latin squares with many subsquares

First, we consider the operation of two Latin squares.

Definition 4.2. (Direct product)

Let A and B be two Latin squares based on $\mathbb{Z}_m$ and $\mathbb{Z}_n$ respectively. Then, the direct product of A and B, denoted by $A \otimes B$ is a Latin square of order mn based on $\mathbb{Z}_m \times \mathbb{Z}_n$ such that the entry $A_{i,j} = x$ is replaced by (x, B) where (x, B) is a Latin square of order n where the (i', j') entry is filed by $(x, B_{i',j'})$.

e.g.

A :

0	1
1	0

, B:

0	1	2
2	0	1
1	2	0

, $A \otimes B$:

(0,0)	(0,1)	(0,2)	(1,0)	(1,1)	(1,2)
(0,2)	(0,0)	(0,1)	(1,2)	(1,0)	(1,1)
(0,1)	(0,2)	(0,0)	(1,1)	(1,2)	(1,0)
(1,0)	(1,1)	(1,2)	(0,0)	(0,1)	(0,2)
(1,2)	(1,0)	(1,1)	(0,2)	(0,0)	(0,1)
(1,1)	(1,2)	(1,0)	(0,1)	(0,2)	(0,0)

,

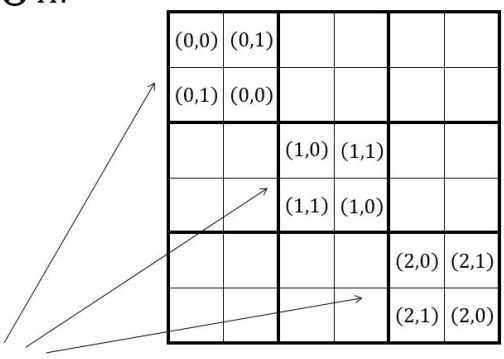
$B \otimes A$:

(0,0)	(0,1)	(1,0)	(1,1)	(2,0)	(2,1)
(0,1)	(0,0)	(1,1)	(1,0)	(2,1)	(2,0)
(2,0)	(2,1)	(0,0)	(0,1)	(1,0)	(1,1)
(2,1)	(2,0)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,1)	(2,0)	(2,1)	(0,0)	(0,1)
(1,1)	(1,0)	(2,1)	(2,0)	(0,1)	(0,0)

B':

0	2	1
2	1	0
1	0	2

$B' \otimes A$:



Latin squares defined on thre disjoint sets.

$B' \otimes A$ is referred to as a Latin square with $\mathbf{2 \times 2}$ holes.

$*$ Let $n = h_1 + h_2 + \cdots + h_t$. If L is a Latin square of order n with t subsquares (as

above) of order $h_1, h_2, \cdots, h_t$ resp. Then, L is a Latin square with holes of type $h_1 \times h_2 \times \cdots \times h_t$.

Problem Construct a Latin square L of order 12, such that L is **commutative** and also with holes of type $\mathbf{2^6}$.

Note If m is odd, then L can be constructed by using direct product. But, for even m, it takes some effort!

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

An example, $m = 4$.

5 Orthogonal Latin Squares.

Definition 5.1. (Orthogonal Latin square)

Two Latin squares of order n based on $\mathbb{Z}_n$ (We use $\mathbb{Z}_n$ throughout of this lecture), $L = [l_{i,j}]$ and $M = [m_{i,j}]$, are orthogonal if $\{(l_{i,j}, m_{i,j}) | 1 \leq i, j \leq n\} = \mathbb{Z}_n^2$, denoted by $L \perp M$.

e.g.

0	1	2
1	2	0
2	0	1

L

$\perp$

0	1	2
2	0	1
1	2	0

M

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

Proposition 5.2. If $L \perp M$, then $\alpha(L) \perp \beta(M)$ for any two permutations α and β of $\mathbb{Z}_n$.

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

Then, we have

1	2	0
2	0	1
0	1	2

$\alpha(L)$

$\perp$

0	2	1
1	0	2
2	1	0

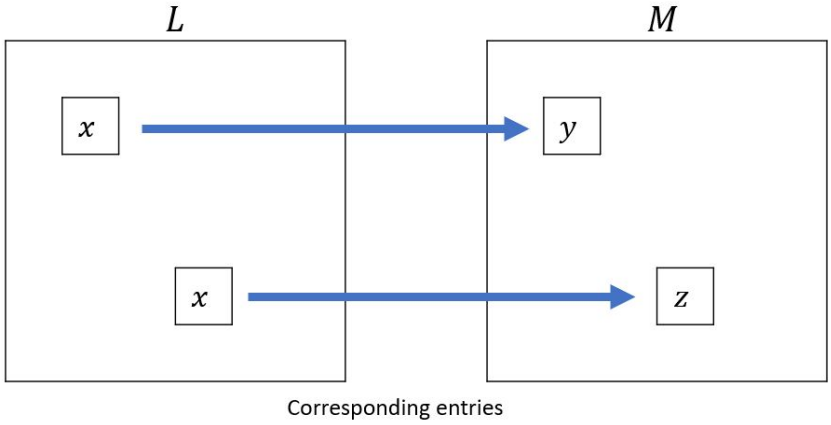
$\beta(M)$

Two Finger's Rule

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

i.e.,

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



Proposition 5.3. If $L_1 \perp L_2$ (of order m) and $M_1 \perp M_2$ (of order n), then $L_1 \otimes M_1 \perp L_2 \otimes M_2$ (of order mn). ($L_1 \perp L_2$, $M_1 \perp M_2$ and $N_1 \perp N_2 \Rightarrow (L_1 \otimes M_1) \otimes N_1 \perp (L_2 \otimes M_2) \otimes N_2$ and more.)

Proposition 5.4. If n is a prime power, the there exist $n-1$ Latin squares of order n which are **mutually orthogonal**.

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

Proof. Since n is a prime power, we have a finite field $GF(n)$, $< F, +, \cdot >$. Let $F^* = F \setminus \{0\}$. For convenience, let $F = \{0 = \alpha_0, \alpha_1, \cdots, \alpha_{n-1}\}$. Now, for $0 \le i, j \le n-1$, we define $L_{i,j}^{(h)} = \alpha_i + \alpha_h \cdot \alpha_j$ where $h \in F^*$. Since $i \ne i'$ implies that $L_{i,j}^{(h)} \ne L_{i',j}^{(h)}$ and $j \ne j'$ implies that $L_{i,j}^{(h)} \ne L_{i,j'}^{(h)}$ where $L^{(h)}$ is a Latin square. As to the orthogonality of two Latin squares, we can also use two fingers rule.

Assume that for $(i,j) \ne (i',j')$, $L_{i,j}^{(h)} = L_{i',j'}^{(h)}$. Consider $1 \le k \ne h \le n-1$. Suppose that $L_{i,j}^{(k)} = L_{i',j'}^{(k)}$. Then we have

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

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

Hence, $L^{(h)} \perp L^{(k)}$. □

Some facts on Finite fields

1. A finite field of order n exists if and only if n is a prime power.

2. $< \mathbb{Z}_n, +, \cdot >$ is a finite field if and only if n is a prime.

3. Let $n = p^m$ where p is a prime and $m \geq 1$. Then a finite field of order n can be constructed by using an irreducible polynomial (over $\mathbb{Z}_p$) $g(x)$ of degree m, that is $GF(n) \cong \mathbb{Z}_p[x]/ < g(x) >$.

4. All finite fields of the same order are isomorphic.

5. If $< F, +, \cdot >$ is a finite field, then $< F^*, \circ >$ is a cyclic group, that is $\langle F^*, \circ \rangle \cong \langle \alpha \rangle$, generated by an element of F^*, α.($F^* = F \setminus \{0\}$.)

6. $x^3 + x + 1$ is irreducible over $\mathbb{Z}_2$. $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$ is a finite field of order 8.

Definition 5.5. (A complete family of MOLS(n))

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

Fact 1.

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

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

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

Observation (Three MOLS(4))

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

$\perp$

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

$? \perp$

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

(Two mutually orthogonal Latin squares of order 4 solve the 16 cards problem!)

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

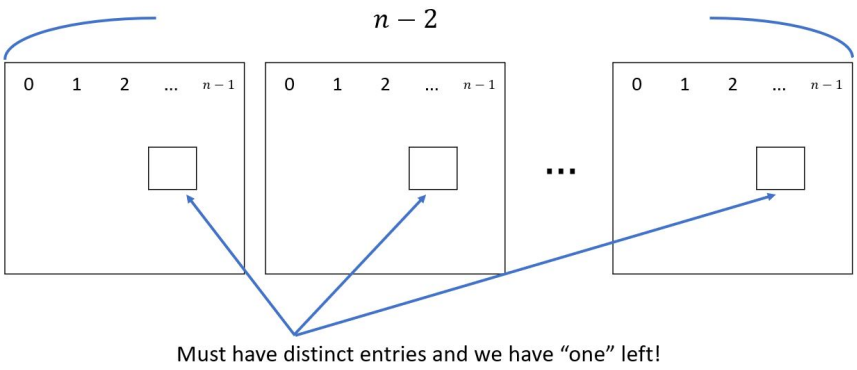
Fact 2.

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

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

Proposition 5.6. If there exist $n-2$ MOLS(n), then we can find $n-1$ MOLS(n).

Idea:



Why "Euler" made the following conjecture?

Euler's Conjecture on MOLS.

For each $n \equiv 2 \pmod 4$, there do not exist two mutually orthogonal Latin squares of order n. (If $n > 1$ and $n \not\equiv 2 \pmod 4$, then either n is a prime or n has a prime factor larger than 2.)

Fact 3. It is not true for $n = 2$ and 6 (only!). Also, $n = 1$ is trivial.

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

Proof. **Case 1.** $n \equiv 0 \pmod 4$: In this case, $n = x^t \cdot m$ where $t \geq 2$ and m is an odd integer. If $m = 1$, then n is a prime power, the proof follows. On the other hand, if $m > 1$, then $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where p_i's are distinct odd primes. Now, by using Proposition 2, we can construct two MOLS(n) by using direct product of two mutually orthogonal Latin squares of order $2^t, p_1^{e_1}, p_2^{e_2}, \cdots, p_k^{e_k}$ respectively. **Case 2.** $n \equiv 1$ or $3 \pmod 4$: The proof of this case has been include in Case 1. □

Problem Prove that there do not exist two mutually orthogonal Latin squares of order 6. (Reference: D. R. Stinson, A short proof of the non-existence of a pair of orthogonal Latin squares of order six, J. Combin. Th. A36, 373-376.)

0	1	2	3	4	5
1	2	3	5	0	4
2	5	0	4	1	3
3	4	1	2	5	0
4	0	5	1	3	2
5	3	4	0	2	1

0	1	2	3	4	5
5	0	4	2	3	1
3	4	1	5	2	0
4	3	5	1	0	2
2	5	3	0	1	4
1	2	0	4	5	3

$(3, 4)$ and $(1, 5)$ are the only two repeated ordered pairs.

Definition 5.7. Two Latin squares of order n defined on the same set S are r-orthogonal if when they are superimposed, exactly r different ordered pairs of S^2 occur among the n^2 ordered pairs of entries. So, the above example is a pair of 34-orthogonal Latin squares of order 6.

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

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

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

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

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

Definition 5.8. (Orthogonal Array)

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

For example, $OA(4, 3)$

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

$\uparrow$

0	0	0
1	①	1
2	2	2

0	1	2
0	①	2
0	1	2

0	1	2
2	⓪	1
1	2	0

0	2	1
2	①	0
1	0	2

Fact 5.

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

Fact 6.

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

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

In application, regularly a partial orthogonal array uses orthogonal array of order m defined of $\mathbb{Z}_n$ with depth k. In such an array, the ordered pairs are required to be distinct, not necessarily be all pairs in $\mathbb{Z}_n^2$. Here, $m \leq n^2$ (as the case in an $OA(k, n)$), but k may be larger than $n+1$. e.g. $n = 3, m = 3, k = 5$

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \\ 0 & 2 & 1 \\ 1 & 2 & 0 \end{bmatrix} \approx \text{Three columns represent three orthogonal partial Latin squares.}$$

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

6 Transversal and Partial Transversal

Definition 6.1. (Transversal)

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

0	(2)	3	1
(3)	1	0	2
1	3	2	(0)
2	0	(1)	3

Definition 6.2. (Partial Transversal)

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

(0)	1	2	3	4	5
1	(2)	0	4	5	3
2	0	1	(5)	3	4
3	4	5	0	(1)	2
4	5	(3)	1	2	0
5	3	4	2	0	1

Fact 1 If $L \perp M$, then both L and M contain transversals. In fact, if L (resp. M) is a Latin square of order n, then L (resp. M) contains n disjoint transversals.

Fact 2 If L is a Latin square of order n where n is odd then $\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} \otimes L$ contains no transversals.

Proof. By a direct checking. □

- Determining whether a Latin square contains a transversal or not is a very difficult problem.

- This problem is equivalent to finding a rainbow perfect matching in an n-edge-colored $K_{n,n}$.
  (Problem) Given examples L' that $\begin{array}{|c|c|}\hline 0 & 1 \\ \hline 1 & 0 \\ \hline \end{array} \otimes L'$ contains a transversal when L' is a Latin square of even order $n = 2m,\ m \in \mathbb{N}$.

Ryser's Conjecture

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

Revised version of Ryser's Conjecture (Brauldi's Conjecture)

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

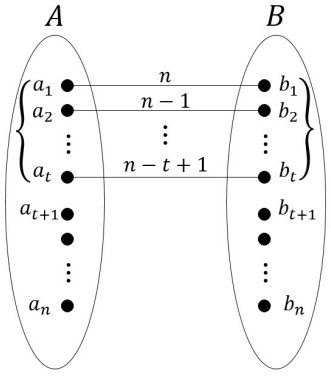
Theorem 6.3. (P. Shor)

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

Theorem 6.4. (D. Woolbright and A.E. Brouwer)

$|T_n| \geq n - \sqrt{n}$.

Proof.

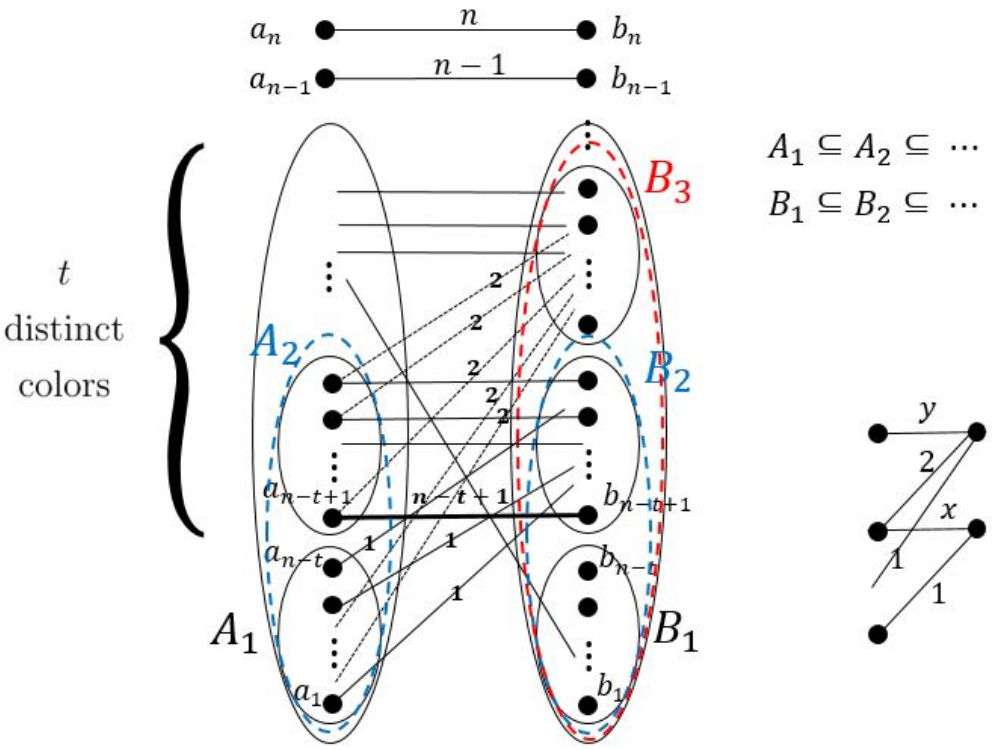


Convert an LS(n) into an n-edge-colored $K_{n,n}$.

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

Consider the color $\mathbf{1}, \mathbf{2}, \cdots, \mathbf{n-t}$ in turn.

Sketch of the proof $|\mathbf{T_n}| \geq \mathbf{n} - \sqrt{\mathbf{n}}$. (D.Woolbright)



(•) $1, 2, \cdots, n-t$ (colors) are missing in $\langle A_1, B_1 \rangle$.

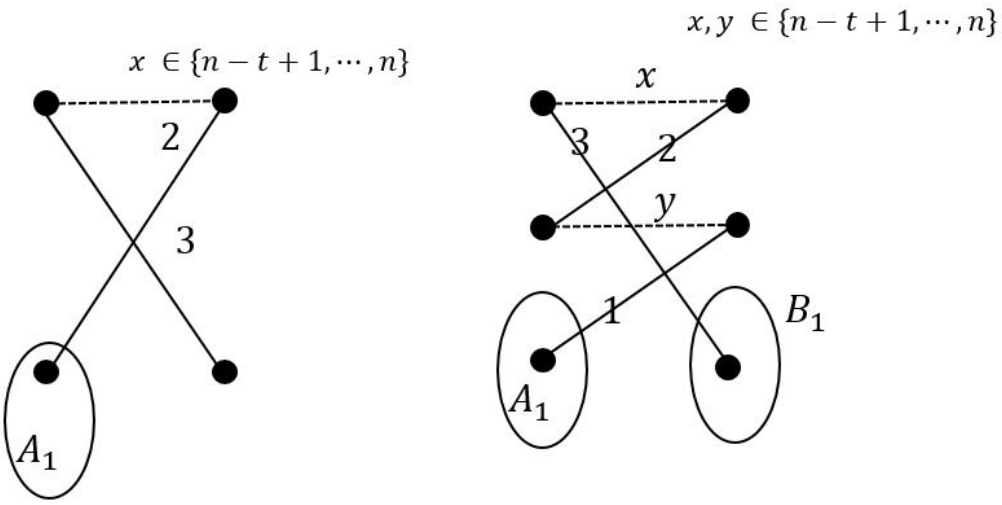
(•) The edges which labeled "1" and incident on the vertices in A_1 are also incident on the vertices in $B_2 \backslash B_1$.

(•) The vertices which colored "2" to "$n-t$" in A_2 are not incident with the vertices in B_1.

(•) Since $2(n-t)$ edges colored "2" in A_2 can not incident on B_1, there are at least $(n-t)$ edges are incident outside B_2 (i.e. $B_3 \backslash B_2$), let $A_3 \backslash A_2$ be correspond vertex set .

(•) The vertices which colored "3" to "$n-t$" in A_3 are not incident on the vertices in B_1.

If the vertices in $A_3 \backslash A_2$ incident on $\langle A_3 \backslash A_2, B_1 \rangle$ colored "3" and above, e.g. "3", then we have 2 conditions:



Observe that the edges colored "3" in A_3 are correspond with $B_4 \backslash B_3$, similarly, the edges colored "$n-t$" in A_{n-t} are corresponding with $B_{n+1} \backslash B_n$, hence

$$n \geq (n-t+1)(n-t) = (n-t)^2 + (n-t) \geq (n-t)^2$$

$$\Rightarrow n - t \leq \sqrt{n},\ t \geq n - \sqrt{n}.$$

□

Progress of finding the size of a partial transversal

(1) $|T| \geq \frac{n}{2}$ (trivial case)

(2) K.K. Koksma (1969, J.C.T 7, 94-95)
$|T_n| \geq \frac{2n-1}{3}$ for $n \geq 7$.

(3) D.A. Drake (1977, J.S.P.I 1, 143-149)
$|T_n| \geq \frac{3n}{4}$. (Simpler method)

(4) S.M.P. Wang (1978, Ph.D. Thesis OSU)
$|T_n| \geq \frac{9n-15}{11}$.

(5) A.E. Brouwer et. al. (1978, Nieuw Archief voor Wiskunde (3) 26, 330-332
D.E. Woolbright (1978, JCTA 24, 235-237)
$|T_n| \geq n - \sqrt{n}$.

(6) P.W. Shor (1982, JCTA 33, 1-8)
$|T_n| \geq n - 5.53(\log_e n)^2 = n - 5.53(\ln n)^2$.

(7) H.L. Fu and Shyh-Chung Lin, (2002, JCMCC 43, 57-64)
$|T_n| \geq n - 5.518(\ln n)^2$. (Using Calculus.)

(8) Erratr of (6), Pooya Hatami and P.W. Shor, (2008, JCTA 115, 1103-1113)
$|T_n| \geq n - O(\ln n)^2$. (Pooya Hatami fixed a bug in (6).)

7 An Introduction of Extremal Set Theory

Under a constraint or a collection of constraints find the maximum number of sets satisfying the given constraints.

$(*)$ Clearly, the collection on of sets, $\mathbb{B}$, from $\mathbb{X}$, is a also design $(\mathbb{X}, \mathbb{B})$.

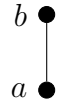
Notations

1. $[n] = \{1, 2, \cdots, n\}$.
2. $\binom{[n]}{k} =_{def}$ the collection of k-subsets (all) of $[n]$.
3. $\binom{n}{k} = |\binom{[n]}{k}|$.
4. $\mathbb{X} = \{x_1, x_2, \cdots, x_n\}$ is a set of n elements and "$\leq$" is a partial order defined on $\mathbb{X}$. $< \mathbb{X}, \leq >$ is called a partial ordered set, Poset in short.

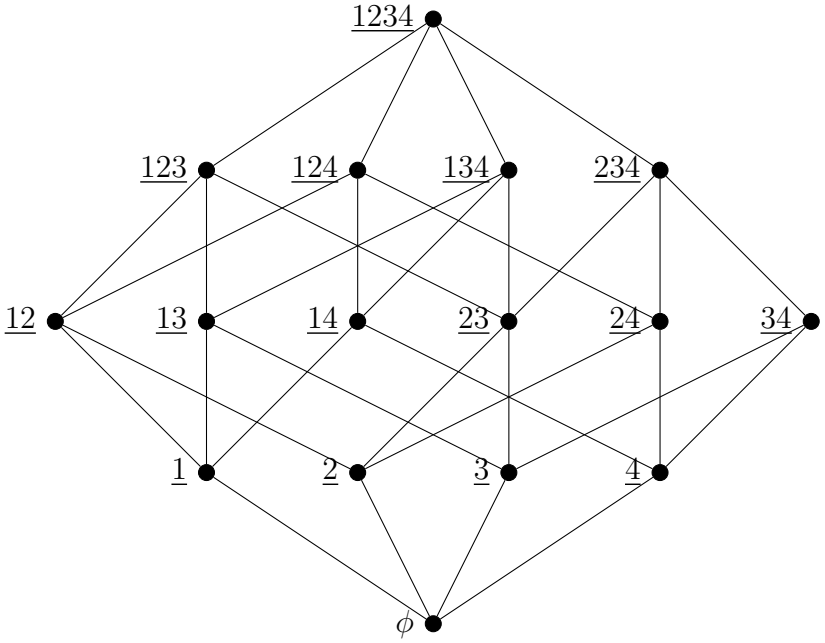
$(*)$ "$\leq$" is a partial order of $\mathbb{X}$ if (i) Reflexivity: $a \leq a \quad \forall a \in \mathbb{X}$, (ii) Anti-symmetry: $a \leq b$ and $b \leq a$ implies that $a = b \quad \forall a, b \in \mathbb{X}$, and (iii) Transitivity: $a \leq b$, $b \leq c$ implies that $a \leq c \quad \forall a, b, c \in \mathbb{X}$.

$(**)$ "$\leq$" is a total order of Y provided any two distinct elements in Y, y_i and y_j, either $y_i \leq y_j$ or $y_j \leq y_i$. (y_i and y_j are comparable.)

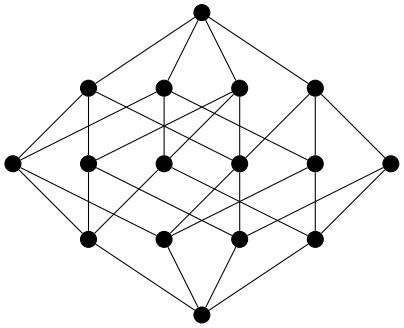
We may use a graph to depict a partial ordered set (Poset), $< S, \leq >$. It is known as the Hasse-diagram. Mainly if $a, b \in S$ and $a \leq b$, than the vertex representing b is higher than a as shown in the following:



So, for example, $< 2^{[4]}, \subseteq >$ can be represented as follows.



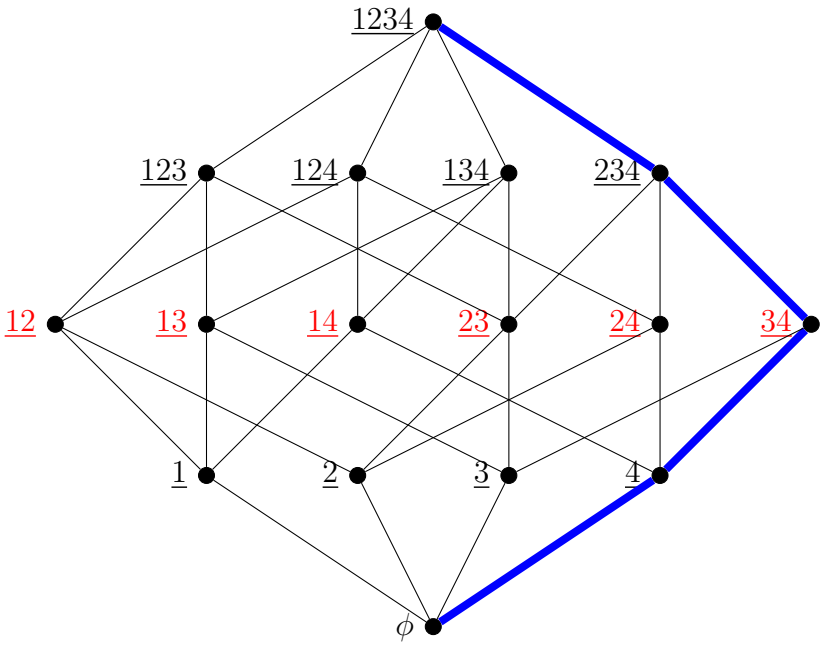
For convenience, this diagram can be considered as a graph:



(*) Only structure will be studied.

(∗) A subset of a poset in which no two distinct are comparable is called an anti-chain. On the other hand, a totally ordered set is called a chain.

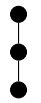
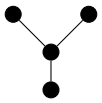
Example (Poset with set-containment)



(The gray vertices are an anti-chain and the darker path is a chain.)

Forbidden poset problem

Given a configuration of posets, say $P_2 = I$:  $(y \leq x)$, find the maximum number of sets in $2^{[n]}$ such that the induced partial ordered set contains no sub-poset which is given. For example, contains no P_2.

$(**)$ We can change $I = P_2$ to any kinds of sub-poset. For example, P_3 :  or 

(Y or S_3, star of order 3).

The result solving P_2 case is known as the Sperner's Theorem.

Theorem 7.1. (**Sperner's Theorem**)

Consider the collection of all subsets of $[n]$. The maximum number of subsets which do not contain each other is equal to $\binom{n}{\lfloor \frac{n}{2} \rfloor}$. (The maximum anti-chain problem.)

Proof. Let $\mathbb{B}$ be a collection of subsets which does not contain each other and attains the maximum. Furthermore, let a_k be the number of sets in $\mathbb{B}$ whose size is k. Hence, $|\mathbb{B}| = \Sigma_{k=0}^{n} a_k$. Note that a_i's may be zero. Since $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$ is clearly an anti-chain, $|\mathbb{B}| \geq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. So, it suffices to prove $|\mathbb{B}| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Claim (Lubell-Yamamoto-Meshalkin, LYM inequality): $\Sigma_{k=0}^{n} a_k / \binom{n}{k} \leq 1$.

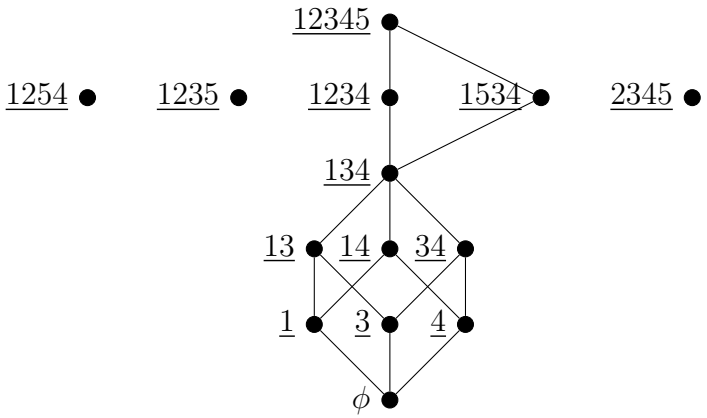
Consider the set of permutations of $[n]$. Clearly, there are $n!$ permutations. Now, for each set $S = \{s_1, s_2, \cdots, s_k\}$ in $\mathbb{B}$, we associate this set with $|S|!(n-|S|)!$ permutations by taking the maximum chain passing $s_1 s_2 \cdots s_k$. ($\phi - s_1' - s_1's_2' - s_1's_2's_3' - \cdots - \underline{s_1 s_2 \cdots s_k} - \underline{s_1 s_2 \cdots s_k s_{k+1}'} - \cdots - [n]$ where $s_i' \in \{s_1, s_2, \cdots, s_k\}$ for $1 \leq i \leq k$.)

Note that each permutation can only be associated with a single set in $\mathbb{B}$. Two sets in $\mathbb{B}$ do not contain each other. Now, we have

$$\Sigma_{S \in A} |S|!(n-|S|)! = \Sigma_{k=0}^{n} a_k \cdot k!(n-k)! \leq n!.$$

This implies that $\Sigma_{k=0}^{n} a_k \cdot \frac{k!(n-k)!}{n!} \leq 1$ and the proof follows.
Since $1 \geq \Sigma_{k=0}^{n} a_k / \binom{n}{k} \geq \Sigma_{k=0}^{n} a_k / \binom{n}{\lfloor \frac{n}{2} \rfloor}$, $\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq \Sigma_{k=0}^{n} a_k = |\mathbb{B}|$. □

e.g. $n = 5$



$(5-3)! \cdot 3!$ maximum chains.

Problem Find the maximum number of subsets in $2^{[n]}$ such that their induced poset does not contain P_3.

A good guess: $\binom{n}{\lfloor \frac{n}{2} \rfloor} + \binom{n}{\lfloor \frac{n}{2} \rfloor + 1}$. (But is it true? Try it!)

Another beautiful result is the maximum collection of sets $B_{n,r}$ of size r which are mutually intersection, that is $\forall S_1, S_2 \in B_{n,r}, \quad S_1 \bigcap S_2 \neq \phi$. $B_{n,r}$ is called an r-uniform intersection family defined on $[n]$.

Theorem 7.2.
$|B_{n,r}| = \binom{n-1}{r-1} \quad \forall n \in \mathbb{N}$. (Erdős–Ko–Rado, EKR theorem)

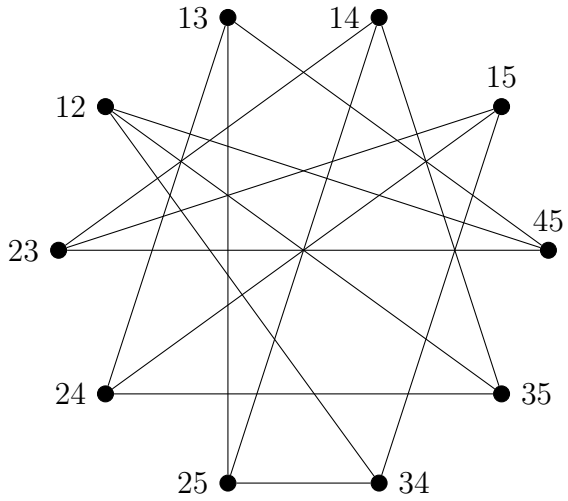
Proof. Let $B = \{S \bigcup \{n\} | S \in \binom{[n-1]}{r-1}\}$. Then, B is an intersection family of $[n]$ since each set contains the element n. Hence, $|B_{n,r}| \geq \binom{n-1}{r-1}$. Next, we prove that $|B_{n,r}| \leq \binom{n-1}{r-1}$.

Observe that if we let $(a_1, a_2, \cdots, a_n)$ be a cyclic permutation of $[n]$, then this cycle contains at most r sets of $B_{n,r}$. For example, $n = 8$ and $r = 3$, let $(3, 1, 8, 2, 7, 5, 6, 4,)$ be an arbitrary cyclic permutation. Now, if $\{8, 2, 7\} \in B_{8,3}$, then we have two more possible sets $\{1, 8, 2\}$ and $\{2, 7, 5\}$. So, for general n, we have at most $r \cdot (n-1)!$ sets for intersecting family. By the same idea in Sperner's Theorem, each set in $B_{n,r}$ can be associated with $r!(n-r)!$ permutations. So, $|B_{n,r}| \cdot r!(n-r)! \leq r(n-1)!$. Therefore $|B_{n,r}| \leq \frac{(n-1)!}{(r-1)!(n-r)!} = \binom{n-1}{r-1}$. □

Example $|B_{7,3}| = \binom{6}{2} = 15$.

Another good problem to study related to sets

Let $n = 2t + 1$. We may define a graph G as follows: $V(G) = \binom{[n]}{t}$ and two vertices are adjacent if and only if their intersection is an empty set. For example, $n = 5, \quad t = 2$



Above graph is in fact the Petersen graph.

$(*)$ The graph G is known as an **odd** graph of order n, denoted by O_n.

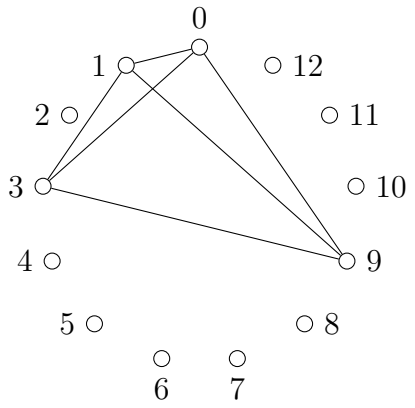
$(**)$ Study the structure of O_n is an important problem in both Graph Theory and Design Theory.

If we further require that any two r-set in $2^{[n]}$ can have at most one element in common, thus exactly one element in common, then the collection of such r-sets denoted by $B_{n,r}^{(1)}$ has at most $\frac{n(n-1)}{r(r-1)}$ sets.

To see this, we notice that any pair of elements in $[n]$ can occur in at most one r-set of $B_{n,r}^{(1)}$. Hence, the pairs we have in total is $\frac{n(n-1)}{2} = \binom{n}{2}$ and each r-set can use $\binom{r}{2} = \frac{r(r-1)}{2}$ pairs, this implies that $|B_{n,r}^{(1)}| \leq \dfrac{\binom{n}{2}}{\binom{r}{2}}$.

In fact, for some n and r, the **equality** does hold.

For example, $B_{7,3}^{(1)} = \{124, 235, 346, 457, 561, 672, 713\}$ (Fano plane) and $|B_{13,4}^{(1)}| = \frac{13\times 12}{4\times 3} = 13$.



$B^{(1)}_{13,4} = \{\{0, 1, 3, 9\} + i \mid i \in \mathbb{Z}_1 3\}$

8 Block Designs

The study of the incidence structures between finite sets is one of the most important topics in Combinatorial Theory. There are there 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 numerical 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.

1. **Notations and preliminaries**

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

- If all the subsets of a design $(\mathbb{X}, \mathbb{B})$ 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 $\mathbb{X} = \{x_1, x_2 \cdots, x_v\}$ 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 $\mathbf{A}$ and also a bipartite graph to represent $(\mathbb{X}, \mathbb{B})$, say $\mathbf{G}_{\mathbb{X},\mathbb{B}}$.

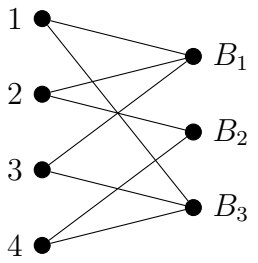
- $A = [a_{i,j}]_{v \times b}$ where $a_{i,j} = \begin{cases} 1, \text{ if } x_i \in B_j, \text{ and} \\ 0, \text{ otherwise.} \end{cases}$
  Therefore, A is a (0,1)-matrix.

- $\mathbf{G}_{\mathbb{X},\mathbb{B}} = (\mathbb{X}, \mathbb{B})$ is a bipartite graph such that $x_i \sim B_j$ if $x_i \in B_j$.

  Example. $\mathbb{X} = \{1, 2, 3, 4\},\ \mathbb{B} = \{\{1, 2, 3\}, \{2, 4\}, \{1, 3, 4\}\}$.

$$\text{A}: \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccc} B_1 & B_2 & B_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}_{4\times 3} \end{array}$$

$\mathbf{G}_{\mathbb{X},\mathbb{B}}$:



  Note: The relation of A and $\mathbf{G}_{\mathbb{X},\mathbb{B}}$ is easy to see. In coding theory the elements in $\mathbb{B}$ can be referred as the set 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.

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

- In an $(\mathbb{X}, \mathbb{B})$, 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 $\{\, |B| \mid B \in \mathbb{B}\}$. If $K = \{k\}$, then we simply use k to denote K.

- (**Definitions**)

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

- 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 $x \in \mathbb{X}$, $r = r_x = \frac{\lambda(v-1)}{k-1}$ which is a constant. Another important fact is $bk = vr$.

- (Only two varieties are concerned!)

- An $(\mathbb{X}, \mathbb{B})$ is called a pairwise balanced design (PBD in short), if any pair of elements in $\binom{\mathbb{X}}{2}$, they occur together in exactly λ blocks of $\mathbb{B}$. Notice that in PBD, the blocks are not necessarily be of the same size. So, it is denoted by 2-(v, K, λ) design where $|\mathbb{X}| = v$.

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

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

  Example $\mathbb{X} = \mathbb{Z}_v$, $\mathbb{B} = \binom{\mathbb{Z}_v}{k}$, $k \geq 2$.

  $(\mathbb{X}, \mathbb{B})$ is a 2-(v, k, λ) design where $\lambda = \frac{r(k-1)}{v-1}$.
  Notice that $r = \binom{v-1}{k-1} = \frac{(v-1)!}{(k-1)!(v-k)!} = \frac{(v-1)(v-2)\cdots(v-k+1)}{(k-1)!}$.
  Hence, $\lambda = \frac{(v-2)(v-3)\cdots(v-k+1)}{(k-1)!} = \binom{v-2}{k-2}$.

- $(\mathbb{X}, \mathbb{B})$ is also a $t - (v, k, \lambda)$ design for all $2 \leq t \leq k < v$.

- The following notions are not related to vector spaces. An $(\mathbb{X}, \mathbb{B})$ is called a **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 $(\mathbb{X}, \mathbb{B})$ is a **linear space** with index 1.

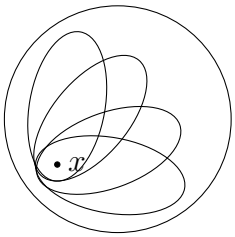
- We can use "Geometry" to refer the above definitions **:**
  Partial linear space **:** Any two lines intersect at most one point.
  linear space **:** Any two points lie on a line (some line) of a partial linear space.

Basic properties of a design

1. If $(\mathbb{X}, \mathbb{B})$ is a 2-(v, k, λ) design, then we have
   (a) for each $x \in \mathbb{X}$, $r_x = r = \frac{\lambda(v-1)}{k-1}$ or $r(k-1) = \lambda(v-1)$.

   (b) $b = |\mathbb{B}| = \frac{\lambda v(v-1)}{k(k-1)}$ or $bk = rv$.

Proof. Since x occurs with (each of) all the other $v-1$ elements exactly in λ blocks, r_x is equal to $\lambda(v-1)$ possible such pairs divided by the $k-1$ pairs which can be obtained from a block.



(The second equality is a consequence of the above idea by using two-way counting.) This concludes the proof of (a).

As to (b), it is a direct counting of the number of pairs occur in $\mathbb{B}$ via the number of pairs occur in a block. Therefore $|\mathbb{B}| = \frac{\lambda\binom{v}{2}}{\binom{k}{2}}$. The second identity comes from the occurrence of elements (total). □

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

Proof. Let A be the incident matrix of $(\mathbb{X}, \mathbb{B})$. 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.

$$AA^T = \begin{array}{c} \\ x_1 \\ \vdots \\ x_v \end{array} \begin{array}{c} \begin{array}{cccc} B_1 & B_2 & \cdots & B_b \end{array} \\ \begin{bmatrix} & & & \\ & & & \\ & & & \end{bmatrix}_{v\times b} \end{array} \begin{bmatrix} & \\ & \\ & \\ & \\ & \end{bmatrix}_{b\times v}$$

Note: $AA^T(i,j)$ 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 ($r_{x_i} = r$) in the blocks of $\mathbb{B}$ and if $i \neq j$, it is the number of blocks in which x_i and x_j occur together in the blocks, λ.

Now, we can find $\mathbf{det(AA^T) = k \cdot r \cdot (r-\lambda)^{v-1}}$. (Gaussian elimination).

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 what follows, we find $\det(AA^T)$ by using its eigenvalues. 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 $\mu\vec{x} = ((r-\lambda) + \lambda u')\vec{x}$. 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, $\det(AA^T) = kr(r-\lambda)^{v-1}$.

Note here that using the spectrum of an adjacency matrix of a graph is one of the main subjects of **Algebraic Graph Theory**.

Theorem 8.1. If $(\mathbb{X}, \mathbb{B})$ is a linear space, then $|\mathbb{X}| \leq |\mathbb{B}|$.

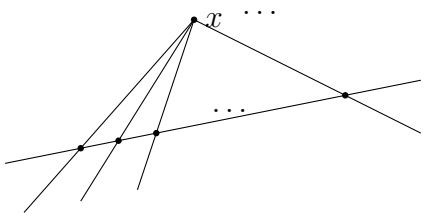
Proof. Again, let $\mathbb{X} = \{x_1, x_2, \cdots, x_v\}$ and $\{B_1, B_2, \cdots, B_b\}$. Since $(\mathbb{X}, \mathbb{B})$ is a linear space, any two elements in $\mathbb{X}$ occur together in a block of $\mathbb{B}$. Assume that $b \leq v$.

Here is an important observation : 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 statements.

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

$$1 = \sum_{x\in\mathbb{X}} \frac{1}{v} = \sum_{x\in\mathbb{X}} \left(\sum_{B\not\ni x} \frac{1}{v(b-r_x)} \right) \tag{b}$$

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



By (a), (b) and (c),

$$\sum_{B\in\mathbb{B}} \left(\sum_{x\notin B} \frac{1}{b(v-|B|)} \right) = \frac{1}{b} \leq \left(\sum_{B\not\ni x} \frac{1}{v(b-r_x)} \right) = \frac{1}{v} \Rightarrow b \geq v.$$

Hence, $b = v$. □

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

(∗∗) $(\mathbb{X}, \mathbb{B})$ is a **projective plane** if $|\mathbb{X}| = |\mathbb{B}|$ and $(\mathbb{X}, \mathbb{B})$ is a **linear space**.

- 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. (Bruck-Ryser-Chowla, 1949 - 1950)

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) $z^2 = (k - \lambda)x^2 + (-1)^{\frac{v-1}{2}} \cdot \lambda y^2$ has a nonzero integral solution when v is odd.

Note that (1) is easy to see $(\det(AA^T) = (\det A)^2 = kr(r - \lambda)^{v-1} = k^2(k - \lambda)^{v-1}$ $(v = b \Rightarrow r = k))$, but the proof of (2) is quite complicate, we omit it.

Special designs related to Geometry

Definition 8.3. (Projective plane and Affine plane)

A Steiner 2-design $S(2, n + 1, n^2 + n + 1) :=$ PG(2,n) is called a projective plane of order n. A Steiner 2-design $S(2, n, n^2)$ is an affine plane of order n, denoted by AG(2,n).

(∗) The existence of a PG(2,n) is "equivalent" to the existence of an AG(2,n).

- A PG(2,n) does exist for each n when n is a prime power.
- No other kind of PG(2,n) has been founded.
- A PG(2,n) does not exist for $n = 1, 2, 6, 10$ and possibly others.

- We can extend AG(2,n) and PG(2,n) to AG(d, n) and PG(d, n) for $d \geq 3$ respectively. But, the constructions are getting harder.

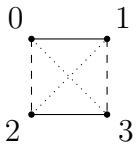
The proof of $(*)$. More details will be given later.

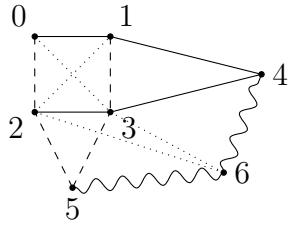
$$\mathrm{PG}(2,n) \overset{\text{Deleting a block.}}{\Longrightarrow} \mathrm{AG}(2,n)$$

$$\mathrm{AG}(2,n) \overset{\text{Adding a line at infinity.}}{\Longrightarrow} \mathrm{PG}(2,n)$$

Examples

$n = 2,\ \mathrm{AG}(2,2):\ \mathbb{X} = \mathbb{Z}_4,\ \mathbb{B} = \Big\{\underbrace{\underline{\{0,1\},\{2,3\}}, \underline{\{1,2\},\{0,3\}}, \underline{\{1,3\},\{0,2\}}}_{\text{parallel classes}}\Big\}.$





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

- A PG(2,n) is a symmetric design, i.e., $|\mathbb{X}| = |\mathbb{B}|$.
- An AG(2,n) contains **parallel classes** each has n blocks. In fact, there are $n+1$ **parallel classes**.
- A parallel class of a design is a collection of blocks $B_1, B_2, \cdots, B_t$ such that $\bigcup_{i=1}^{t} B_i = \mathbb{X}$.

9 BIBD with $k = 3$

(·) A 2-(v,2,λ) design exists for all $v \geq 2$.

This is a direct consequence of using $\lambda \cdot K_v$.

(·) A 2-(v,3,1) design exists if and only if $v \equiv 1$ or 3 (mod 6).

This theorem was first proved by T.P. Kirkman in 1847. Later, there are many different proofs for this seeming easy but quite complicate "fact".

Theorem 9.1.

A 2-(v,3,1) design, known as a Steiner triple system of order v, exists if and only if $v \equiv 1$ or 3 (mod 6).

Proof. ($\Rightarrow$) As mentioned earlier, if a 2-(v,3,1) design exists then $r = \frac{v-1}{3-1} = \frac{v-1}{2}$ and $b = \frac{v(v-1)}{6}$ are both integers. This implies that $v \equiv 1$ or 3 (mod 6).
($\Leftarrow$)We prove this sufficient condition by constructing a 2-(v,3,1) design for each $v \equiv 1$ or 3 (mod 6).

Kirkman's 15 School Girls Problem

Problem: Arrange 15 girls to line up in five rows with each row has three girls to walk to school. If we can complete that any two of girls stay in a row for some day in seven days?

Answer: We need at least 7 days since each day we use up 15 pairs and in total there are $\binom{15}{2} = 105$ pairs. So, the extra requirement is that every day, the arrangement is in fact a parallel class. Such designs are also known as Kirkman triple systems. Such systems of order v exist if and only if $v \equiv 3$ (mod 6) except $v = 9$.

Note $AG(2,3)$ is a Kirkman triple system of order 9. Here is an answer of 15 girls problem.

0	1	2	0	3	4	0	5	6	0	7	8	0	9	10	0	11	12	0	13	14
3	7	11	1	7	9	1	8	10	1	11	16	1	12	13	1	3	5	1	4	6
4	9	13	2	12	14	2	11	13	2	4	5	2	3	6	2	8	9	2	7	10
5	10	12	5	8	13	3	9	14	3	10	13	4	8	11	4	10	14	3	8	12
6	8	14	6	10	11	4	7	12	6	9	12	5	7	14	6	7	13	5	9	11

First, we need to construct Steiner triple systems of small orders, $v = 7, 9, 13$ and 15. (Defined on $\mathbb{Z}_v$)

$v = 7$ 013, 124, 235, 346, 450, 561, 602 $(PG(2))$

$v = 9$ 012, 345, 678, 036, 147, 258, 048, 156, 237, 057, 138, 246 $(AG(3))$

$v = 13$ $\mathbb{B} = \{(0,3,4)+i, (0,2,7)+i \pmod{13} \mid i \in \mathbb{Z}_{13}\}$ $(PG(3))$

$v = 15$ $\mathbb{B} = \{(0,3,4)+i, (0,2,8)+i, (0,5,10)+i \pmod{15} \mid i \in \mathbb{Z}_{15}\}$

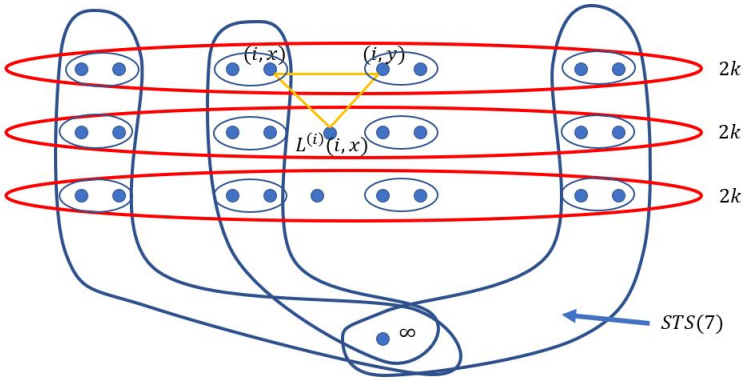
Now, we shall use the following two constructions to construct all the other Steiner triple systems of order v, $STS(v)$ in short.

Case 1. $v \equiv 1 \pmod 6$, $v \geq 19$.

Let $v = 6k+1$, $k \geq 3$. Let $L^{(i)}$ be a commutative Latin square of order $2k$ defined on $\{(i,j) | i \in \mathbb{Z}_3 \text{ and } j \in \mathbb{Z}_{2k}\}$ with holes of size 2. Let $(\mathbb{X}, \mathbb{B})$ be a design with $\mathbb{X} = \{\infty\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$, and $\mathbb{B}$ be defined as follows:

(a) $B \in \mathbb{B}$ if B is a block in an $STS(7)$ defined on $\{\infty, (i,2h), (i,2h+1) \mid i \in \mathbb{Z}_3\}$ for each $0 \leq h \leq k-1$; and

(b) $\{(i,x),(i,y),(i+1, L^{(i)}(x,y))\} \in \mathbb{B}$ for all $i \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$ such that (i,x) and (i,y) are met in a 2×2 hole. (The first component is taking modulo 3 and the second component is taking modulo $2k$.)



It's left to check that (𝕏,𝔹) is an $STS(v)$. First, we count $|\mathbb{B}|$. Since each entry outside the hole and in the upper part of $L^{(i)}$ gives a triple(block), we have $3\cdot\frac{(2k)^2-(2k)\cdot 2}{2}+7k$ which is equal to $\frac{12k^2-12k+14k}{2} = 6k^2+k = \frac{1}{6}(6k+1)6k = \frac{v(v-1)}{6}$. Hence, if each pair of two elements in $\mathbb{X}$ occurs, then the pair occurs at most once. So, we have to verify each pair of elements of $\mathbb{X}$ does occur in a block of $\mathbb{B}$ defined above in (a) and (b). Clearly, if one of the elements is ∞, then $\{\infty, x\}$ occurs in the blocks defined in (a). On the other hand, consider (i_1, x) and (i_2, x) where $i_1, i_2 \in \mathbb{Z}_3$ and $x, y \in \mathbb{Z}_{2k}$. First, if they are in the holes of either $L^{(i_1)}$ or $L^{(i_2)}$ $(=L^{(i)})$, then they occur together in the block of (a). On the other hand, if they are not in the holes of $L^{(i)}$, then we have two cases to consider:

(1) $i_1 = i_2 = i$

Clearly, they occur together in $\{(i,x),(i,y),(i+1, L^{(i)}(x,y)\}$ in (b).

(2) $i_1 \neq i_2$

Without loss of generality, let $i_2 \equiv i_1 + 1 \pmod 3$ and $i_1 = i$. Since there exists a $z \in \mathbb{Z}_{2k}$ such that $L^{(i)}(x,y) = y$,(i_1, x) and (i_2, y) will occur in $\{(i_1,x),(i_1,z),(i_2,y)\}$ of (b).

This concludes of proof. All $STS(v)$'s of order $v \equiv 1 \pmod 6$ have been constructed. Next, let $v \equiv 3 \pmod 6$ and $\mathbb{X} = \{\infty_1, \infty_2, \infty_3\} \cup (\mathbb{Z}_3 \times \mathbb{Z}_{2k})$.

The construction can be obtained similarly. The blocks in $\mathbb{B}$ can be defined as follows: (a) Use $STS(9)$ instead of $STS(7)$ when $\{\infty\}$ is replace by $\{\infty_1, \infty_2, \infty_3\}$. Moreover, fix $\{\infty_1, \infty_2, \infty_3\}$ as a block for each $STS(9)$. (b) Use the same construc-

tion.

Hence $|\mathbb{B}| = 1 + 11k + \frac{3[(2k)^2-4k]}{2} = 6k^2 + 5k + 1 = (2k+1)(3k+1) = \frac{(6k+3)(6k+2)}{6} = \frac{v(v-1)}{6}$. And the existence of every pair of distinct elements in $\mathbb{X}$ is similar. □

Note that the above construction was obtained not long time ago. There are quite a few methods in construction Steiner triple systems. One of the most "popular" one is called "cyclic construction" method or in general, difference method.

Definition 9.2. (Difference)

Let $\mathbb{X} = \mathbb{Z}_n$. Then the difference of two distinct elements x and y in $\mathbb{X}$ is $\pm(x-y) := \pm|x-y|$ such that $1 \le |x-y| \le \lfloor \frac{n}{2} \rfloor$.

The differences obtained in a set S is the set of all difference of two distinct elements in S.

Example

$S = \{0,1,3\} \subseteq \mathbb{Z}_7$. $\text{diff}(S) = \{\pm 1, \pm 2, \pm 3\} \pmod 7 = \{1,2,3,4,5,6\}$.

Difference Sets

Given a subset S of $\mathbb{Z}_n$. The set of differences is S, denoted by $D_2(S)$, is $\{a-b \pmod n | a,b \in S\}$. For example, if $n = 7$ and $S = \{1,2,4\}$, then $D(S) = \{1,2,3,4,5,6\}$. Moreover, if $n = 13$ and $S = \{1,2,4,9\}$, then $D(S) = \{1,2,\cdots,12\}$.

(·) Observe that if $a, b \in S \subseteq \mathbb{Z}_n$, then $a - b \pmod n \in \mathbb{Z}_n^*$ provided $a \neq 6$.

(·) If $|S| = s$, then $|D(S)| \le 2\binom{s}{2}$ (procided $s \le n$).

(·) A set S is called an equi-difference set if the elements of S form an arithmetic progresion, i.e., $S = \{a, a+d, \cdots, a+(k-1)d\}$ where $a + (t-1)d \le n$ and $d > 0$.

(·) Note that an equi-difference set could produce the minimum number of distinct differences among all the sets of the same cardinality.

(·) If the difference of a and b is defined as $\min\{|a-b|, n-|a-b|\}$, then it is known as the circular difference of a and b or half-difference in short.

(·) $\{1,2,4\}$ in $\mathbb{Z}_7$ will provide three half-differences $1, 2$ and 3. Clearly, in $\mathbb{Z}_n$, the

set of half-differences will be $\{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$.

(·) The set of half-differences in S is defined as $D_2(S)$. Moreover, $|D_2(S)| \leq \binom{|S|}{2}$.

(·) Again, an equi-difference set S is the set whose $D_2(S)$ is of "smaller" cardinality. For example, $D(\{1, 2, 3, 4\}) = \{1, 2, 3\}$ and $D(\{0, 2, 4, 6\}) = \{2, 4\}$ in $\mathbb{Z}_8$.

Definition 9.3. (Difference set)

A set of k elements $D = \{a_1, a_2, \cdots, a_k\}$ in $\mathbb{Z}_v$ is called a (v, k, λ)-difference set if $\forall d \in \mathbb{Z}_v^*$ there are exactly λ ordered pairs (a_i, a_j), $a_i, a_j \in D$ such that $a_i - a_j \equiv d \pmod{v}$.

Definition 9.4. (Base blocks)

A collection of subsets of $\mathbb{X} = \mathbb{Z}_v$ is called a set of base blocks $\mathbb{C}$ of a 2-(v, k, λ) design if the following conditions satisfied:

(1) Each set of $\mathbb{C}$ is of size k; and

(2) $\bigcup_{S \in \mathbb{C}} \text{diff}(S)$ contains each difference in $\pm\{1, 2, \cdots, \lfloor \frac{n}{2} \rfloor\}$ exactly λ times.

Constructing design cyclically

Theorem 9.5. If $\mathbb{C}$ is a set of base blocks of a 2-(v, k, λ) design $(\mathbb{X}, \mathbb{B}) = (\mathbb{Z}_v, \mathbb{B})$, then $\mathbb{B} = \{i + S | S \in \mathbb{C} \text{ and } i \in \mathbb{Z}_v\}$. (Note that if $S = \{x_1, x_2, \cdots, x_k\}$, then $i + S = \{x_1 + i, x_2 + i, \cdots, x_k + i\} \pmod{v}$.)

Example

$\mathbb{X} = \mathbb{Z}_7$, $\mathbb{C} = \{\{0, 1, 3\}\}$ is a set of base block of an $STS(7)$.

Example

$\mathbb{X} = \mathbb{Z}_{15}$, $\mathbb{C} = \{\{0, 3, 4\}, \{0, 2, 8\}, \{0, 5, 10\}\}$ is a set of base blocks of an $STS(15)$. Note that $\{0, 3, 4\}$ and $\{0, 2, 8\}$ generate 15 blocks resp. and $\{0, 5, 10\}$ generates 5 blocks.

Definition 9.6. (Full orbit and short orbit)

A base block is of full orbit (short orbit) if the block generates v blocks (less than v blocks) in $(\mathbb{Z}_v, \mathbb{B})$ respectively.

Definition 9.7. (Cyclic design)

A design is called a cyclic design if the design can be obtained by using a set of base blocks.

$(*)$ The above $STS(7)$ and $STS(15)$ are cyclic Steiner triple systems.

$(**)$ No cyclic $STS(9)$ exists!

Theorem 9.8.

A cyclic Steiner triple system of order $v \neq 9$ exists.

In order to prove the above theorem, we need to find a set of base blocks for each order $v \equiv 1$ or 3 (mod 6). Therefore, a systematic construction should be obtained.

Definition 9.9. (Skolem sequences)

A Skolem sequence of order n is a sequence of length $2n$ $(a_1, a_2, \cdots, a_{2n})$ such that each of the elements in $\{1, 2, \cdots, n\}$ occurs exactly twice. Moreover, the indices of "i", $i \in \{1, 2, \cdots, n\}$, occurred exactly "$i$" apart, i.e. if $a_t = i$, then either $a_{t+i} = i$ or $a_{t-i} = i$.

Example

$n = 4, < 1, 1, 3, 4, 2, 3, 2, 4 >$

$a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8$.

$n = 5, < 1, 1, 3, 4, 5, 3, 2, 4, 2, 5 >$.

Theorem 9.10.

A Skolem sequence of order n exists if and only if $n \equiv 0, 1$ (mod 4). (Type A)

For $n \equiv 2$ or 3 (mod 4), we can obtain an extended Skolem sequence by using one extra bit. For example, $n = 2, < 1, 1, 2, -, 2 >$. $n = 3, < 1, 1, 2, 4, 3, -, 3 >$.

Theorem 9.11.

An extended Skolem sequence of order n exists if and only if $n \equiv 2$ or $3 \pmod 4$. (Type B)

For convenience, we can also use their indices of a Skolem sequence or an extended Skolem sequence to represent the sequence. For example, $< 1,1,3,4,5,3,2,4,2,5 >:= \{\{1,2\},\{7,0\},\{3,6\},\{4,8\},\{5,10\}\}$ and $< 1,1,2,3,2,-,3 >:= \{\{1,2\},\{3,5\},\{4,7\}\}$. Therefore, they are partitions of $[1,10]$ and $[1,7] \setminus \{6\}$ into five 2-subsets and three 2-subsets respectively.

For convenience, we shall use set-notation for Skolemn sequences. So, we hace a revised definition for Skolemn sequence.

Definition 9.12.

A Skolemn sequence of order n is a partition of $[1,2n,]$ into 2-subsets $\{\{a_i,b_i\}|i = 1,2,\cdots,n\}$ such that $|a_i - b_i| = i, 1 \le i \le n$. An extended Skolemn sequence of order n is a partition of $[1,2n+1] \setminus \{2n\}$ into 2-subsets $\{\{a_i,b_i\}|i = 1,2,\cdots,n\}$ such that $|a_i - b_i| = i, 1 \le i \le n$.

Fact. A Skolemn sequence of order n exists if $n \equiv 0$ or $1 \pmod 4$. An extended Skolemn sequence of order n exists if $n \equiv 2$ or $3 \pmod 4$.

The constructions for Skolemn sequences and extended Skolemn sequences

Let $n \ge 6$. Case 1 and case 2 are for Skolemn sequences. The others are for extended Skolemn sequences. Case 1: $n \equiv 0 \pmod 4$. Let $n = 4k$.

	Pairs	Differences
$r = 1,2,\cdots,2k$	$\{4k+r-1, 8k-r+1\}$	$\{4k-2r+2\}\{2,4,\cdots,4k\}$
$r = 1,2,\cdots,k-2$	$\{r, 4k-r-1\}$	$\{4k-2r-1\} \cup \{2k+3,\cdots,4k-3\}$
$r = 1,2,\cdots,k-2$	$\{k+r+1, 3k-r\}$	$\{2k-2r-1\} \cup \{3,\cdots,2k-3\}$
	$\{k-1,3k\},\{k,k+1\},$ $\{2k,4k-1\},\{2k+1,6k\}$	$\{2k+1,1,2k-1,4k-1\}$

Case 2: $n \equiv 1 \pmod 4$. Let $n = 4k + 1$.

	Pairs	Differences
$r = 1, 2, \cdots, 2k$	$\{4k + r + 1, 8k - r + 3\}$	Check yourself!
$r = 1, 2, \cdots, k$	$\{r, 4k - r + 1\}$	
$r = 1, 2, \cdots, k - 2$	$\{k + r + 2, 3k - r + 1\}$	
	$\{k + 1, k + 2\}, \{2k + 1, 6k + 2\}, \{2k + 2, 4k + 1\}$	

Case 3: $n \equiv 2 \pmod 4$. Let $n = 4k + 2$.

	Pairs	Differences
$r = 1, 2, \cdots, 2k$	$\{r, 4k - r + 2\}$	Check yourself!
$r = 1, 2, \cdots, k - 1$	$\{4k + r + 3, 8k - r + 4\}$	
$r = 1, 2, \cdots, k - 1$	$\{5k + r + 2, 7k - r + 3\}$	
	$\{2k + 1, 6k + 2\}, \{4k + 1, 6k + 3\},$ $\{4k + 3, 8k + 5\}, \{7k + 3, 7k + 4\}$	

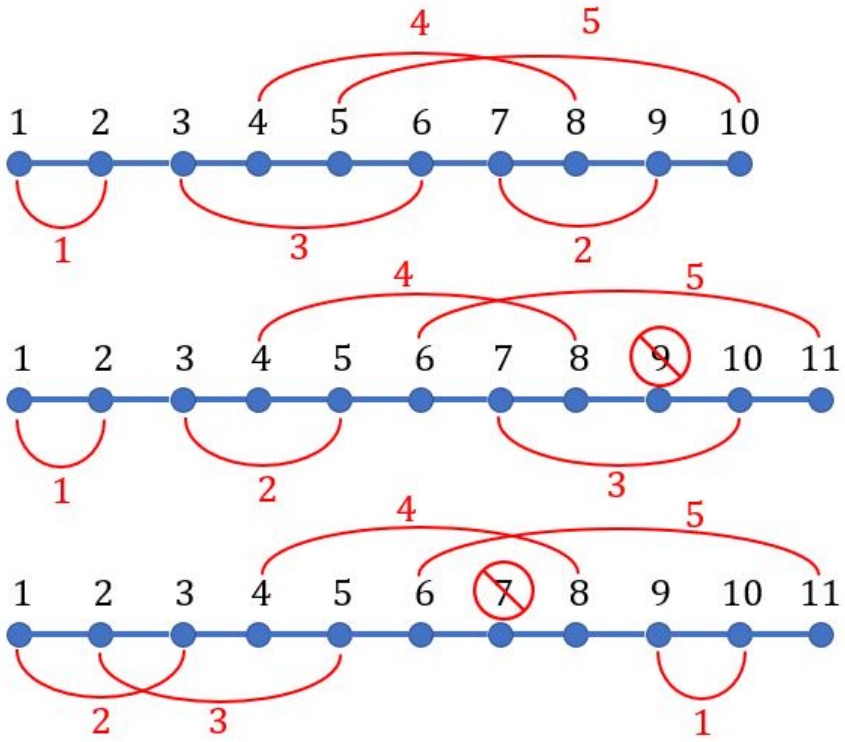
Case 4: $n \equiv 3 \pmod 4$. Let $n = 4k - 1$.

	Pairs	Differences
$r = 1, 2, \cdots, 2k - 2$	$\{4k + r, 8k - r - 2\}$	Check yourself!
$r = 1, 2, \cdots, k - 2$	$\{r, 4k - r - 1\}$	
$r = 1, 2, \cdots, k - 2$	$\{k + r + 1, 3k - r\}$	
	$\{k - 1, 3k\}, \{k, k + 1\}, \{2k, 4k - 1\},$ $\{2k + 1, 6k - 1\}, \{4k, 8k - 1\}$	

Fact. For each $d \in \mathbb{N}$, $[i + d, 2n + d]$, a Skolemn sequence of order n exists if $n \equiv 0$ or $1 \pmod 4$. This is also true for extended Skolemn sequence on $[1 + d, 2n + d + 1] \setminus \{2n + d\}$.

In fact, there are quite a few modified sequences by using the above two sequences.

For example,

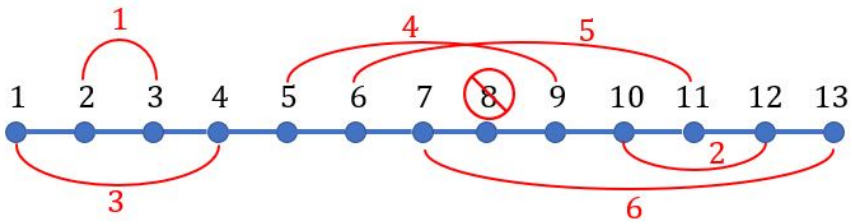


Fact. $[1, 2n+1] \setminus \{k\}$ can be partitioned into 2-subsets $\{\{a_i, b_i\} | i = 1, 2, \cdots, n\}$ such that $|a_i - b_i| = i$ for each $1 \leq i \leq n$ provided,

(a) $n \equiv 0$ or $1 \pmod 4$ and $k \equiv 1 \pmod 2$; and

(b) $n \equiv 2$ or $3 \pmod 4$ and $k \equiv 0 \pmod 2$.

For example,



Theorem 9.13.

A cyclic $STS(v)$ exists if and only if $v \neq 9$ and $v \equiv 1$ or 3 (mod 6).

Proof.

Case 1: $v \equiv 1 \pmod 6$. For convenience, let $v = 6k+1$ and we consider the "half" difference. Then, the set of differences is $\{1, 2, \cdots, 3k\}$. Note that the difference $3k$ is the same as the difference $3k+1$. Hence, by using Skolemn sequences of type A or type B, $\{k+1, k+2, \cdots, 3k\}$ or $\{k+1, k+2, \cdots, 3k-1, 3k+1\}$ can be partitioned (respectively) into 2-subsets $\{\{a_i, b_i\} | i = 1, 2, \cdots, k\}$, such that $|a_i - b_i| = i$, $i = 1, 2, \cdots, k$. This implies that we can find k base blocks $\{0, i, i + a_i = b_i\} (a_i < b_i)$ for $i = 1, 2, \cdots, k$. Thus, we have a cyclic $STS(v)$.

Example $v = 19$, differences are $1, 2, 3, \cdots, 9$.

$4, 5, 6, 7, 8, 10 \Rightarrow (4, 5), (6, 8), (7, 10)$

$\Rightarrow$ Difference triples are $\{1, 4, 5\}, \{2, 6, 8\}, \{3, 7, 10\}$.

Base blocks: $\{0, 1, 5\}, \{0, 2, 8\}, \{0, 3, 10\}$.

Case 2: $v \equiv 3 \pmod 6$. Let $v = 6k+3$ and the set of half differences is $\{1, 2, \cdots, 3k+1\}$. First, we delete $2k+1$ form the above set. Hence, the set of differences is $\{1, 2, \cdots, k, k+1, k+2, \cdots, 2k, 2k+2, \cdots, 3k+1\}$. It remains to show that $\{k+1, k+2, \cdots, 2k, 2k+2, \cdots, 3k+1\}$ can be partitioned into 2-subsets $\{a_i, b_i\}$ such that $|a_i - b_i| = b_i - a_i = i$ $(b_i > a_i)$ for

$i = 1, 2, \cdots, k$. Again, it can be done by using either $3k+1$ or $3k+2$ in respective cases. In fact, it is up to the relationship between k and v. If $k \equiv 1$ or $2 \pmod 4$, then we partition $\{k+1, k+2, \cdots, 3k, 3k+2\} \setminus \{2k+1\}$ into suitable 2-sets provided $k \equiv 0$ or $1 \pmod 4$. On the other hand, if $k \equiv 3$ or $0 \pmod 4$, then we partition $\{k+1, k+2, \cdots, 3k+1\} \setminus \{2k+1\}$ into 2-subsets satisfying $|a_i - b_i| = b_i - a_i = i$ $(b_i > a_i)$. □

Recursive Constructions

We may also use the idea of recursion to construct all $STS(v)$. There are two constructions.

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

Since $v \equiv 1$ or $3 \pmod 6$, K_{v+1} is a complete graph of even order and thus K_{v+1} can be decomposed into v 1-factors by way of $\chi'(K_{v+1}) = v$. Let $F_1, F_2, \cdots, F_v$ be the set of 1-factors mentioned above. Now, we are ready to constuct an $STS(2v+1) = (\mathbb{Z}_{2v+1}, \mathbb{B})$. Let the given $STS(v)$ be defined on $\{0, 1, 2, \cdots, v\}$ and $V(K_{v+1}) = \{v, v+1, \cdots, 2v\}$. Moreover, let $F_i = \{\{a_1^i, b_1^i\}, \cdots, \{a_{\frac{v+1}{2}}^i, b_{\frac{v+1}{2}}^i\}$ be the ith 1-factor, $i = 1, 2, \cdots, v$. So, $\mathbb{B}$ can be obtained by the following:

(a) If B is a triple (block) in $STS(v)$, then $B \in \mathbb{B}$; and

(b) For each $i \in \{0, 1, 2, \cdots, v-1\}$, $\{i, a_j^{(i+1)}, b_j^{(i+1)}\} \in \mathbb{B}$ where $\{a_j^{(i+1)}, b_j^{(i+1)}\} \in \mathbb{F}_{i+1}$.

(We use $< i, \mathbb{F}_{i+1} >$ denote $\{i, a_j^{(i+1)}, b_j^{(i+1)}\}$ for convenience.)

It is a routine matter to check that $(\mathbb{X}, \mathbb{B}) = (\mathbb{Z}_{2v+1}, \mathbb{B})$ is an $STS(2v+1)$.

2. $v \to 2n+7$

This construction is more complicate comparing to the first one. The main idea comes from the graph $K_{v+7} \approx G(v+7; D)$ where $D = \{1, 2, \cdots, \frac{v+7}{2}\}$. We can view K_{v+7} as a circulant graph with difference set D. By Stern and Lenz's Lemma, $G := K_{v+7} \setminus G(v+7, \{1, 2, 3\})$ can be v-edge-colored for each $v \geq 3$. This implies that G can be decomposed into v 1-factors $F_1, F_2, \cdots, F_v$. Now, we are ready to construct an $STS(2v+7)$ by way of an $STS(v)$ defined on $\mathbb{X} = \{0, 1, 2, \cdots, v-1\}$. Let $(\mathbb{X}, \mathbb{B}_1)$ be an $STS(v)$ and $STS(2v+7) = (\mathbb{Z}_{2v+7}, \mathbb{B})$. It suffices to find $\mathbb{B}$. The triples of $\mathbb{B}$ are obtained as follows:

(a) $\forall B \in \mathbb{B}_1$, $B \in \mathbb{B}$;

(b) Decompose $G(v+7;\{1,2,3\})$ into K_3's defined on $\{v, v+1, \cdots, 2v+6\}$ and let each of them be a triple of $\mathbb{B}$; and

(c) $< i, \mathbb{F}_{i+1} > \subseteq \mathbb{B}$ for each $i = 0, 1, \cdots, v-1$. ($< i, \mathbb{F}_{i+1} >$ is similar to (b) in case 1.)

Again, it is not difficult to check $(\mathbb{Z}_{2v+7}, \mathbb{B})$ is indeed an $STS(2v+7)$.

Based on the above two constructions, we conclude the proof by showing each $STS(u)$ can be obtained by recursive constructions $v \to 2v+1$ or $v \to 2v+7$. First, if $u = 6t+1$, then $u = 12s+1$ or $12s+7$. Since $12s+1 = (6s-3) \times 2 + 7 \equiv 3 \times 2 + 7 \pmod 6$ and $12s+7 = (6s+1) \times 2 + 1$, an $STS(u)$ can be constructed recursively. On the other hand, if $u = 6t+3$, then $u = 12s+3$ or $12s+9$. Since $12s+3 = (6s+1) \times 2 + 1$ and $12s+9 = (6s+1) \times 2 + 9$, an $STS(u)$ can be constructed by the same reason. This concludes the proof. □

Theorem 9.14. (Stern and Lenz)

Let $G(n;D)$ be a circulant graph with difference set D. If $\frac{n}{2}$ is an integer and $\frac{n}{2} \in D$, then $G(n;D)$ is of class 1.

This theorem can be applied to prove the will-known Doyen-Wilson theorem on Steiner triple systems.

Theorem 9.15. (Doyen and Wilson, 1973)

An $STS(v)$ adn be embedded in an $STS(u)$ if and only if $u \geq 2v+1$.

Proof. ($\Rightarrow$) Let $(\mathbb{X}_1, \mathbb{B}_1)$ be an $STS(v)$ and $(\mathbb{X}, \mathbb{B})$ be an $STS(u)$ such that $\mathbb{X}_1 \in \mathbb{X}$, say x_0. Then, for each element $x_i \in \mathbb{X}_1$, the triple contain x_0 and x_i should be $\{x_0, x_i, y_i\}$ where $y_i \in \mathbb{X} \setminus \mathbb{X}_1$. Since there are v elements in $\mathbb{X}+1$, $\mathbb{X} \setminus \mathbb{X}_1$ contains x_0, y_i, $i = 1, 2, \cdots, v$. Hence, $u \geq 2v+1$.

($\Leftarrow$) It takes some effort to finish the proof.

Case 1. $v = 6k+1$ and $u = 6h+3$ where $u \geq 12k+3$, i.e. $h \geq 2k$.

By the idea of recursive constructions, we define a complete graph G of order

$u - v = 6(h-k) + 2$ defined on $[0, u-1] \setminus [0, v-1]$. Therefore, $G \cong G(u-v; D)$ where $D = \{1, 2, \cdots, 3(h-k)+1\}$. Now, G can be decomposed into v 1-factors and a collection of triples. See the following example to deseribe the idea.

Example $v = 13$, $u = 45$.

$G := G(32; \{1, 2, \cdots, 16\})$. Let $D' = \{9, 11, 12, 13, 14, 15, 16\}$. By Stern and Lenz's lemma, $G(32; D')$ can be partitioned into 13 1-factors. On the other hand $G(32; \{1, 2, 3, 4, 5, 6, 7, 8, 10\})$ can be partitioned into cyclic triples by using extended Skolem sequence.

Case 2. $v = 6k + 3$ and $u = 6h + 3$ where $u \geq 12k + 7$, i.e. $h \geq 2k + 1$.

Example $v = 15$, $u = 45$. $G := G(30\{1, 2, \cdots, 15\}$

Now, $D' = \{6, 8, 9, 11, 12, 13, 14, 15\}$, $D_1 = \{10\}$ (short orbit), $D_2 = \{1, 2, 3, 4, 5, 7\}$ (full orbits). $G(30; D')$ can be partitioned into 15 1-factors and $G(30; D_1 \cup D_2)$ can be decomposed into triples.

Case 3. $v = 6k + 1$ and $u = 6h + 1$

Example $v = 13$, $u = 43$.

$(\cdot)$ $G(30; \{1, 2\})$ can be decomposed into 10 triangles, B_0, and one Hamilton cycle (two 1-factors), let them be F_1 and F_2.

Let $D' = \{5, 8, 12, 13, 14, 15\}$. Together with F_1 and F_2 and $G(30; D')$, we hace 13 1-factors. For the other differences D" $= \{3, 4, 6, 7, 9, 11\} \cup \{10\}$. $G(30; D$") can be decomposed into triangles, $\mathbb{B}_{\not\vdash}$. Combine $\mathbb{B}_0, \mathbb{B}_1$, $STS(13)$ and $(a_i F_i)$'s we have the embedding.

Case 4. $v = 6k + 3$ and $u = 6h + 1$

The proof is similar to that of case 3. □

10 Constructing Designs Using Latin Squares

To start, we use a well-known construction to construct an STS(v) where $v \equiv 3 \pmod 6$. Let $v = 6k+3$ and $L = [l_{i,j}]$ be an idempotent commutative Latin square of order $2k+1$. Now, we are ready to construct the Steiner triple system of order $6k+3$.

(1) Let $\mathbb{X} = \mathbb{Z}_3 \times \mathbb{Z}_{2k+1}$.

(2) $\forall i \in \mathbb{Z}_{2k+1}$), let $\{(0,i),(1,i),(2,i)\} \in \mathbb{B}$.

(3) $\forall i < j \in \mathbb{Z}_{2k+1}$, let $\{(0,i),(0,j),(1,l_{i,j})\}$, $\{(1,i),(1,j),(2,l_{i,j})\}$, $\{(2,i),(2,j),(0,l_{i,j})\}$ be triples in $\mathbb{B}$.

Then, $(\mathbb{X},\mathbb{B})$ is an STS($6k+3$).

It is easy to check any two elements of $\mathbb{X}$ will occur in a triple and we have in total $(2k+1) + 3 \cdot \frac{(2k+1)^2-(2k+1)}{2} = 2k+1+6k^2+3k = 6k^2+5k+1 = \frac{(6k+3)(6k+2)}{6}$.

($*$) If $(\mathbb{X},\mathbb{B})$ is an STS(v), then $|\mathbb{B}| = \frac{v(v-1)}{6}$.

($**$) In difference method, the part $v \equiv 3 \pmod 6$ is comparatively more complicate, we can replace it with this construction if we only try to prove the "sufficient" direction.

We can use MOLS(n) to construct designs with larger blocks.

($***$) An Affine plane of order n exists if n is a prime power.

Step 1 Construct $n-1$ MOLS(n), let them be $L^{(1)}, L^{(2)}, ..., L^{(n-1)}$.

Step 2 Let $L^{(r)}$ and $L^{(c)}$ be the row-indices and column-indices squares respectively.

$L^{(r)} =$

1	1	$\cdots$	1
2	2	$\cdots$	2
		$\vdots$	
n	n		n

$L^{(c)} =$

1	1		1
2	2		2
$\vdots$	$\vdots$	$\cdots$	$\vdots$
n	n		n

Step 3 Let $\overline{\mathbb{X}} = (\mathbb{Z}_n \cup \{\infty\}) \times \mathbb{Z}_n = \mathbb{X} \cup (\{\infty\} \times \mathbb{Z}_n)$.

Step 4 $\forall i \neq j \in \mathbb{Z}_n$, let $\overline{B_{i,j}} = \{(0,i),(1,j),(2,L^{(1)}(i,j)),(3,L^{(2)}(i,j)),\cdots,$ $(\infty, L^{(n-1)}(i,j))$ be a block in $\overline{\mathbb{B}}$. (There are n^2 blocks.)

Step 5 Let $\mathbb{B}' = \{\overline{B}_{i,j} - (\infty, L^{(n-1)}(i,j))|\ \overline{B}_{i,j} \in \overline{\mathbb{B}}\}$.

Step 6 Let $\mathbb{B} = \mathbb{B}' \cup \{\{i\} \times \mathbb{Z}_n|\ i \in \mathbb{Z}_n\}$.

Then, we conclude the $(\mathbb{X}, \mathbb{B})$ is an Affine plane of order n.

- Let $\widetilde{\mathbb{X}} = \{\{\infty\}\} \cup \overline{\mathbb{X}}$ and $\widetilde{\mathbb{B}} = \overline{\mathbb{B}} \cup \{\{\{\infty\}, \{i\} \times \mathbb{Z}_n\}|\ i \in \mathbb{Z}_n\}$.
  Then $(\widetilde{\mathbb{X}}, \widetilde{\mathbb{B}})$ is a projective plane of order n.

We can also use an orthogonal array to construct the desired projective plane of order n where n is a prime power. The steps are similar, except the k^{th} block B_k will be obtained by using the k^{th} column vector of the following array.

$$\mathrm{A}: \begin{array}{c} \overset{B_k}{\overset{\downarrow}{\begin{bmatrix} & i & \\ & j & \\ \cdots & L_{i,j}^{(1)} & \cdots \\ & \vdots & \\ & L_{i,j}^{(n-1)} & \end{bmatrix}}} \\ {\scriptstyle (n+1)\times n^2} \end{array}$$

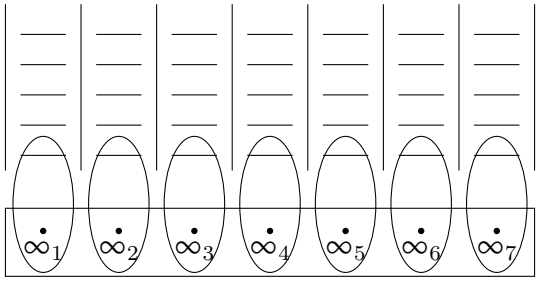
If the entries of A are in $\{1,2,\cdots,n\}$, then we have $B_k = \{i, n+j, 2n+L_{i,j}^{(1)}, \cdots, n^2+L_{i,j}^{n-1}\}$. So, by adding $\{0,1,2,\cdots,n\}, \{0,n+1,n+2,\cdots,2n\}, \cdots, \{0,n^2+1,n^2+2,\cdots,n^2+n\}$ to the collection of n^2 blocks $B_k's$ we obtain the PG(n). Now, an AG(n) can be constructed by deleting $\{0,n^2+1,n^2+2,\cdots,n^2+n\}$ and keep those blocks $B_k' = B_k \backslash \{0,n^2+1,n^2+2,\cdots,n^2+n\}$.

Here, we mention some PBD's.

Theorem 10.1. For each $v \equiv 1 \pmod 3$, there exists a 2-$(v,K,1)$ design where $K = \{4,7\}$ except $v = 10, 19$.

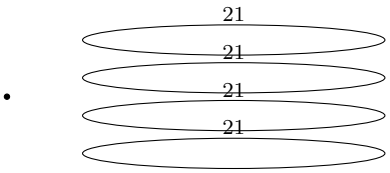
We omit the proof, but we present some examples here.

$v = 22$



By using a Kirkman triple system of order 15, we can attach 7 points in the "infinity" and obtain the desired PBD.

$v = 85$



First, we have a $2-(85,\{4,22\},1)$ design by using two MOLS(21). Then, a $2-(85,\{4,7\},1)$-design will be obtain from $v = 22$ case.

We can also use MOLS(n) to construct PBDs in which K is of size larger than one. For example, we can use an Affine plane of order 5 to construct a PBD 2=(24,{4, 5},1) design: $(\mathbb{X},\mathbb{B})$. The idea comes from deleting an element from $\mathbb{X}$. Then, each block which contains this element be comes a block of size 4, and the other blocks which do not contain this element remain the same.

Hence, we can start with a special type of design, and then either adding or deleting elements (to or from) $\mathbb{X}$ to obtain a new design.

Definition 10.2. (Group Divisible Designs of type n^m)

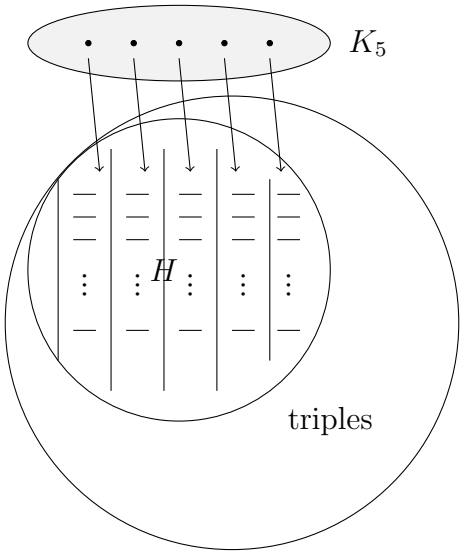
A design $(\mathbb{X},\mathbb{B})$ is called a group divisible design of type n^m if $\mathbb{X}$ can be partitioned in m disjoint subsets of size n (called groups) $G_1, G_2, \cdots, G_m$ such that each $B \in \mathbb{B}$, $|B \cap G_i| \leq 1$, $|B| = k$ and every pair of two elements from different groups occurs together in exactly λ blocks of $\mathbb{B}$. The design $(\mathbb{X},\mathbb{B})$ is denoted by GDD$(n, m; k, \lambda)$.

A GDD$(n, m; k, \lambda)$ can be stated as a ***k*-GDD of type n^m and index λ**. We shall solve the case $k = 3$ and $\lambda = 1$ in what follows. First, we need a theorem.

Theorem 10.3. For each $v \equiv 5 \pmod 6$, a 2-$(v, \{3, 5\}, 1)$ design exists. Moreover, we have such a design with exactly one block of size 5.

Proof. (By difference method.) Let $v = 6k + 5$ and $\mathbb{X} = \mathbb{X}_1 \cup \mathbb{X}_2$ where $|\mathbb{X}_1| = 5$ and $|\mathbb{X}_2| = 6k$. Now let $\mathbb{X}_2 = \mathbb{Z}_{6k}$. Hence, the set of differences in $\mathbb{Z}_{6k} = \{1, 2, \cdots, 3k(\text{half})\}$. As mentioned in the above construction, we can find difference triples either in $\{1, 2, \cdots, 3k-3\}$ or $\{1, 2, \cdots, 3k-4, 3k-2\}$. Hence, after taking away those triples, we have a 5-regular graph H left defined on $\mathbb{Z}_{6k}$. Since $3k$ is one of the differences, $\chi'(H) = 5$. The proof then follows by the same idea as in recursive construction.

□



Note. Such a PBD also exists for $v \equiv 1$ or $3 \pmod 6$ since we can take all blocks of size 3.

Group Divisible Design (3-GDD)

Problem For which m and n, $k_3|K_{m(n)}$?

Fact 1 If $n = 1$, then $m \equiv 1$ or $3 \pmod 6$.

Definition 10.4. (3-sufficient)

A graph G is said to be 3-sufficient if (1) $|G| \geq 3$, (2) G is an even graph and (3) $3 \Big| \|G\|$.

Problem (Open) For which 3-sufficient graph G, $K_3|G$?

Nash-Williams Conjecture (Remains open)

If G is 3-sufficient and $\delta(G) \geq \frac{3}{4}|G|$, then $K_3|G$.

Fact 2 If $K_{m(n)}$ is 3-sufficient, then

(1) Either n is even or n is odd and m is odd; and

(2) $3 \Big| \binom{m}{2} \cdot n^2$.

Theorem 10.5. If $K_{m(n)}$ is 3-sufficient and $m \geq 3$, then $K_3|K_{m(n)}$.

We need several basic facts in order to prove the theorem.

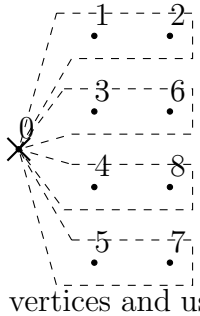
Fact 3 $K_3|K_{3(n)}$. (By using a L.S. of order n.)

Fact 4 $K_3|K_{4(n)}$ if and only if n is even.

Proof. ($\Rightarrow$) Since $m = 4$, n must be even in order that each vertex is of even degree.

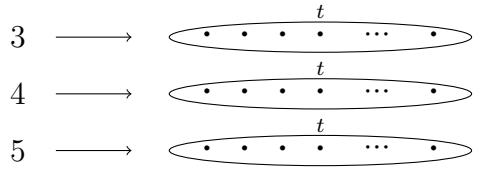
($\Leftarrow$) If $n = 2$, then $K_3|K_{4(2)}$. This is a consequence of deleting one vertex of an STS(9).

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



Now, let $n = 2t$. The proof follows by blowing up each vertex into t vertices and use an LS(t) to construct all the $K_3's$ we need.

For example,



As a consequence, we have $8t^2$ $K_3's$ in total. This is also the number $K_3's$ we desire : $\frac{6\cdot(2t)^2}{3} = 8t^2$.

Fact 5 If $m \equiv 1$ or $3 \pmod 6$, then $K_3|K_{m(n)}$ for each positive integer n.

Proof. It is a direct consequence of blowing each vertex of K_n into n vertices. □

Fact 6 If $m \equiv 0$ or $4 \pmod 6$ and n is even, then $K_3|K_{m(n)}$.

Proof. First, we take an STS($2m+1$) $(\mathbb{X}, \mathbb{B})$ and delete one vertex from $\mathbb{X}$, then we have $K_3|K_{m(2)}$. Since n is even, we use the same technique as that in Fact 4. This concludes the proof. □

Fact 7 If $m = 5$ and $3 \,|\, n$, then $K_3|K_{m(n)}$.

Proof. Let $n = 3k$. By the fact taht $K_3|K_{5(3)}$, we conclude the proof by blowing each vertex into k vertices. □

Fact 8 If $m \equiv 5 \pmod 6$ and $3 \,|\, n$, then $K_3|K_{m(n)}$.

Proof. This is a direct result of the existence of a PBD $(m, \{3, 5\}, 1)$-design and Fact 7. □

Fact 9 If $m \equiv 2 \pmod 6$ and $6 \,|\, n$, then $K_3|K_{m(n)}$.

Proof. Let $m = 6k + 2$. Consider $2m + 1 \equiv 5 \pmod 6$. Since a $(2m + 1, \{3, 5\}, 1)$-design exists, we may let it be as in the following figure.

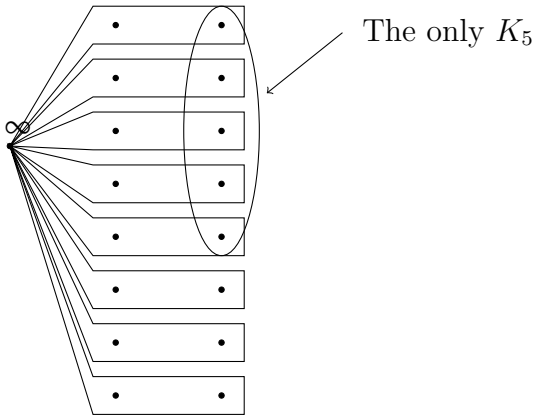


Figure for $(2m+1,\{3,5\},1)$ PBD

Now, by deleting ∞, we obtain a decomposition of $K_{m(2)}$ into $K_3's$ and one K_5. Let $n = 6k$. Then, the proof follows by blowing up each vertex into $3k$ vertices. □

Theorem 10.6. (3-GDD)

$K_3|K_{m(n)}$ if and only if $m \geq 3$ and $K_{m(n)}$ is 3-sufficient.

Proof. Combining Facts 5, 6, 7, 8, 9; we have the proof. □

11 Disproof of Euler's Conjecture

Definition 11.1. (Transversal Designs)

A $GDD(n, m; m, \lambda)$ is also known as a transversal design $T(n; m, \lambda)$, i.e. each block is of size m (the number of groups) or each block $B \in \mathbb{B}$ intersects each group.

$(\cdot)$ Observation

The existence of a pair of orthogonal Latin squares of order n is equivalent to the existence of a $T(n; 4, 1)$ design.

$(*)$ If we can construct a $T(n; m, 1)$, then there exist $m-1$ MOLS(n).

$(\cdot)$ Since a $T(n; n+1, 1)$ exists for prime power n, there exist $n-1$ MOLS(n). The existence of $T(n; n+1, 1)$ can be proved by a consequence of $PG(n)$: Delete an element say "0" and then keep all the blocks of size $n+1$.

Another idea of constructing MOLS(n) comes from the construction of $PBD(\mathbb{X}, \mathbb{B})$, where $|\mathbb{X}| = n$.

Theorem 11.2.

Let $(\mathbb{X}, \mathbb{B})$ be 2-$(n, K, 1)$ design such that for each $k \in K$, there exist at least t mutually orthogonal Latin squares of order k. Then, there exist $t-1$ MOLS(n).

Proof. If for each $k \in K$, there exists an idempotent Latin square of order k, then there exists an idempotent Latin square of order n which is obtained from $(\mathbb{X}, \mathbb{B})$, see next page for an example. Therefore, if there are at least $t-1$ idempotent mutually orthogonal Latin squares of order k for each $k \in K$, then we can construct $t-1$ idempotent Latin squares of order n.

$(*)$ (A consequence of the existence of t MOLS(k)'s.)

By the fact that all induced subsquares from blocks are orthogonal, there $t-1$ Latin squares of order n are also mutually orthogonal by two finger's rule. □

$\mathbb{X} = \{0, 1, 2, \cdots, 9\}$,

$\mathbb{B} = \{0123, 0456, 0789, 147, 258, 369, 159, 267, 348, 168, 249, 357\}$

L :

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

a	c	b
c	b	a
b	a	c

a	c	d	b
d	b	a	c
b	d	c	a
c	a	b	d

$(*)$ If $\{i, j\}$ occurs in B_k, then use the idempotent Latin square defined on B_k to fill in $L_{i,j}$ or $L_{j,i}$ respectively.

Conclusion

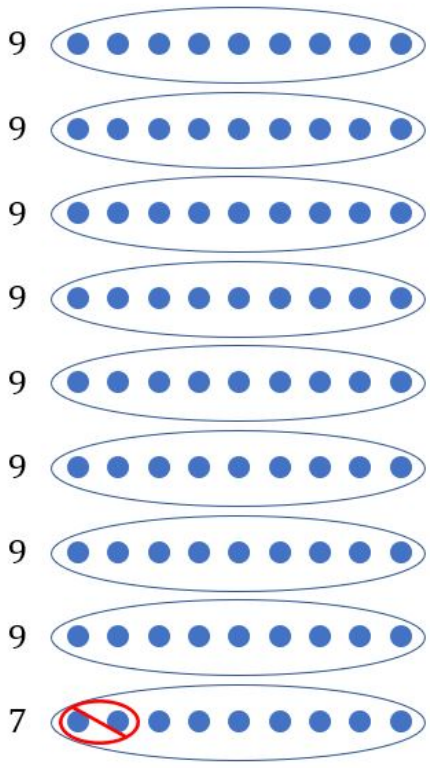
(i) If $i = j$, then $L_{i,j} = i$.

(ii) If $i \neq j$, $L_{i,j}$ is an element of B_k where $\{i, j\} \subseteq B_k$.

(iii) $L_{i,j} \neq L_{i,j'}$ and $L_{i,j} \neq L_{i',j}$. ($\{i, j\}$ and $\{i, j'\}$,respectively $\{i, j\}$ and $\{i', j\}$ are not in the same block.)

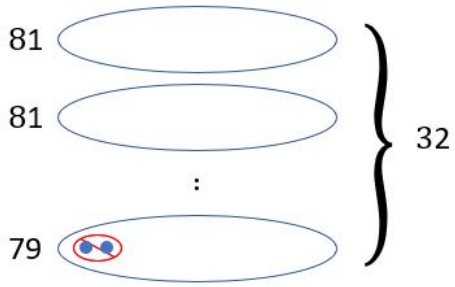
Since a 2-$(22, \{4, 7\}, 1)$ design exists, there exists a pair of MOLS(22). In fact, for each $v \geq 19$ and $v \equiv 7$ and 10(mod 12), a 2-$(v, \{4, 7^*\}, 1)$ design exists where 7^* means that K_7 occurs exactly once. Hence, pair of MOLS(v) exists for $v \equiv 7$ and 10(mod 12) and $v \geq 19$.

$(*)$ We can use a 2-$(v, \{7, 8, 9\}, 1)$ design for certain v's to show that five MOLS(v) exist. For example, $v = 70$.



Start with the $AG(9)$ and truncate two elements from the last block.

Another example, $v = 2590$. A PBD with $\lambda = 1$



Let $(\mathbb{X}, \mathbb{B}) = GD(81, 32; 32, 1) \cong T(81, 32, 1)$. Truncate two elements from the last

group and take groups as blocks. Then, we have a PBD, 2-$(2590, \{31, 32, 79, 81\}, 1)$ design. This implies that there are at least "29" MOLS(2590)'s where $2590 = 2 \times 1295$.

Construction of $T(3m + u; 4, 1)$ where (i) a $T(m; 5, 1)$ exists, (ii) a $T(u; 4, 1)$ exists and (iii) $m \geq u$.

Step 1. Let $(\mathbb{X}_1, \mathbb{B}_1)$ be a $T(m; 5, 1)$ with five groups G_1, G_2, G_3, G_4, G_5 and $(\mathbb{X}_2, \mathbb{B}_2)$ be a $T(u; 4, 1)$ with four groups $H_i = \{x_1, x_2, \cdots, x_u\} \times \{i\}, \quad i = 1, 2, 3, 4$, i.e. $H_i = \{(x_1, i), (x_2, i), \cdots, (x_u, i)\} := \{x_{1,i}, x_{2,i}, \cdots, x_{u,i}\}$.

Step 2. Let $(\mathbb{X}'_1, \mathbb{B}'_1)$ be the $T(m; 4, 1)$ obtained by trancating G_5. Hence, $\mathbb{B}'_1$ can be partitioned into in parallel classes $L_1, L_2, \cdots, L_u, \cdots, L_m$ where each L_j is a set of m disjoint blocks of size 4 defined on $\mathbb{X}_1 \setminus \mathbb{G}_5 = \mathbb{X}'_1$. ($|\mathbb{X}'_1| = 4m$, $|\mathbb{B}'_1 = m^2$.)

Step 3. Let $\mathbb{X}$ be defined as follows:

$\bar{G_1}$: $G_1 \times \{1\}, G_1 \times \{2\}, G_1 \times \{3\}, H_1$

$\bar{G_2}$: $G_2 \times \{1\}, G_2 \times \{2\}, G_2 \times \{3\}, H_2$

$\bar{G_3}$: $G_3 \times \{1\}, G_3 \times \{2\}, G_3 \times \{3\}, H_3$

$\bar{G_4}$: $G_4 \times \{1\}, G_4 \times \{2\}, G_4 \times \{3\}, H_4$

Noticed that each group contains $3m + u$ elements.

Step 4. Choose u parallel classes from $(\mathbb{X}'_1, \mathbb{B}'_1)$, say $L_1, L_2, L_3, \cdots, L_u$. Starting from $L_1 = \{B_{1,1}, B_{2,1}, \cdots, B_{m,1}\}$, use $(B_{i,1} \times \{1, 2, 3\}) \cup \{x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}\}$ to construct a $T(4 : 4, 1)$ which contains the block $\{x_{1,1}, x_{1,2}, x_{1,3}, x_{1,4}\}$. Then in L_2, use $(B_{i,2} \times \{1, 2, 3\}) \cup \{x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4}\}$ to construct a $T(4; 4, 1)$ which contains the block $\{x_{2,1}, x_{2,2}, x_{2,3}, x_{2,4}\}$. So, we have $12m \cdot u$ blocks in total without using $\{x_{j,1}, x_{j,2}, x_{j,3}, x_{j,4}\} \quad j = 1, 2, \cdots, u$.

Step 5. For those blocks $B' = \{a, b, c, d\}$ in $L_{u+1} \cup L_{u+2} \cup \cdots \cup L_m$, we use $\begin{Bmatrix} (a,1), (a,2), (a,3) \\ (b,1), (b,2), (b,3) \\ (c,1), (c,2), (c,3) \end{Bmatrix}$ to construct a $T(3; 4, 1)$ for each blocks. In total, we have

$9(m-u)\cdot m$ blocks.

Step 6. Construct a $T(u;4,1)$ based on $\cup_{j=1}^{u} H_j$. In total, we have u^2 blocks. Combining Steps 4 - 6, we have $15mu + 9m^2 - 9um + u^2 = 9m^2 + 6mu + u^2 = (3m+u)^2$.

Step 7. Step 6 shows that the total numbers of pairs from different groups we have is $6(3m+u)^2$. We have to claim every pair from different groups occurs in a block in Step 4 - 6. It can be done by a routine check. □

(•) Note that u can be 1, since two MOLS(1) exist.

(•) The choice of m's is interesting. If $m \equiv 1$ or $5 (\text{mod } 6)$, then there exist at least three MOLS(m)'s.

(••) Let $n \equiv 2i (\text{mod } 18)$, $i = 0, 1, 2, \cdots, 8$.

Then $n = 18k + 2i$ for $k \geq 1$.

n	m	u	
$18k$	$6k-1$	3	
$18k+2$	$6k-1$	5	
$18k+4$	$6k+1$	1	
$18k+6$	$6k+1$	3	
$18k+8$	$6k+1$	5	
$18k+10$	$6k+1$	7	
$18k+12$	$6k+1$	9	$k \geq 2; k = 1 \Rightarrow 30 = 3 \cdot 9 + 3$
$18k+14$	$6k+1$	11	$k \geq 2; k = 1 \Rightarrow 30 = 3 \cdot 9 + 5$
$18k+16$	$6k+5$	1	

Theorem 11.3. (P. B. S., 1959) [1][2]

For each $n \neq 2, 6$, there exists a pair of MOLS(n).

Proof. Combining the results obtained above. □

[1] Parker, E. T. "Orthogonal Latin Squares." Proc Natl Acad Sci U S A (1959): 860-61. PubMed Central. Web. 1 Apr. 2016.

[2] Bose, R. C., and S. S. Shrikhande. "On the Construction of Sets of Mutually Orthogonal Latin Squares and the Falsity of a Conjecture of Euler." Trans. Amer. Math. Soc. Transactions of the American Mathematical Society 95.2 (1960): 191-209. Web. 18 Mar. 2016.

Two mutually orthogonal Latin squares of order 10.

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

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

Two mutually orthogonal Latin squares of order 14.

12	7	0	6	4	2	11	9	13	5	3	1	10	8
1	11	10	4	5	6	13	8	9	0	7	12	2	3
2	1	11	0	7	12	3	4	5	6	13	8	9	10
10	9	8	1	2	3	4	5	6	13	0	7	12	11
7	0	12	3	1	10	8	6	4	2	11	9	13	5
3	2	1	13	8	9	10	11	0	7	12	4	5	6
5	4	3	10	11	1	2	0	7	12	6	13	8	9
13	6	5	2	3	4	0	7	12	8	9	10	11	1
9	8	13	5	6	0	7	12	10	11	1	2	3	4
11	10	9	8	0	7	12	1	2	3	4	5	6	13
0	12	7	11	9	13	5	3	1	10	8	6	4	2
4	3	2	7	12	5	6	13	8	9	10	11	1	0
6	5	4	12	13	8	9	10	11	1	2	3	0	7
8	13	6	9	10	11	1	2	3	4	5	0	7	12

12	13	4	10	7	0	1	9	6	3	11	8	5	2
9	8	10	5	6	7	4	13	12	11	1	2	3	0
5	0	6	7	8	9	10	11	1	2	3	4	13	12
6	5	7	1	2	3	0	4	13	12	8	9	10	11
4	12	13	6	3	11	8	5	2	10	7	0	1	9
1	11	2	9	10	4	13	12	3	0	5	6	7	8
0	3	5	2	4	13	12	6	7	8	9	10	11	1
7	6	8	4	13	12	9	10	11	1	2	3	0	5
10	9	11	13	12	1	2	3	0	5	6	7	8	4
2	1	3	12	0	5	6	7	8	9	10	11	4	13
13	4	12	3	11	8	5	2	10	7	0	1	9	6
8	7	9	11	1	2	3	0	5	6	4	13	12	10
11	10	1	0	5	6	7	8	9	4	13	12	2	3
3	2	0	8	9	10	11	1	4	13	12	5	6	7

12 On the construction of 2-(v, 4, 1) designs

Small cases

2-(13, 4, 1) design ≈ projective plane of order 3.

2-(16, 4, 1) design ≈ Affine plane of order 4.

Lemma 12.1. For each $n \geq 17,\ n \neq 28,\ n \equiv 0$ or 1 (mod 4), there exists a pairwise balanced GDD with five (or four) groups $G_1,\ G_2,\ G_3,\ G_4,\ G_5$ such that $|G_1| = |G_2| = |G_3| = |G_4| = r,\ |G_5| = r_1 \equiv 0$ or 1 (mod 4), $0 \leq r_1 \leq r$ and all blocks are of size **4** or **5**. Moreover, a T(r, 5, 1) exists.

Proof. We use $< r,\ r,\ r,\ r,\ r_1 >$ to denote the sizes of groups.

17,20,21,...

$24 \to < 5,\ 5,\ 5,\ 5,\ 4 >$

$25 \to < 5,\ 5,\ 5,\ 5,\ 5 >$

$28 \to < 7,\ 7,\ 7,\ 7,\ 0 >$

$29 \to < 7,\ 7,\ 7,\ 7,\ 1 >$

$32 \to < 7,\ 7,\ 7,\ 7,\ 5 >$

$33 \to < 8,\ 8,\ 8,\ 8,\ 1 >$

$36 \to < 8,\ 8,\ 8,\ 8,\ 4 >$

$37 \to < 9,\ 9,\ 9,\ 9,\ 1 >$

$40 \to < 9,\ 9,\ 9,\ 9,\ 4 >$

$41 \to < 9,\ 9,\ 9,\ 9,\ 5 >$

$44 \to < 9,\ 9,\ 9,\ 9,\ 8 >$

$45 \to < 9,\ 9,\ 9,\ 9,\ 9 >$

$48 \to < 11,\ 11,\ 11,\ 11,\ 4 >$

$49 \to < 11,\ 11,\ 11,\ 11,\ 5 >$

$52 \to < 13,\ 13,\ 13,\ 13,\ 0 >$

$53 \to < 13,\ 13,\ 13,\ 13,\ 1 >$

For $n \geq 52,\ n = 4r + r_1$ where $0 \leq r_1 \leq r$ and $r_1 \equiv 0$ or 1 (mod 4) such a pairwise balanced GDD does exist since there are at least three MOLS(r) for each order $r > 10$. □

Lemma 12.2. If a 2-(v, 4, 1) exists, then $v \equiv 1$ or 4 (mod 12).

Proof. It follows by $3 \,|\, v - 1$ and $6 \,\big|\, \binom{v}{2}$. □

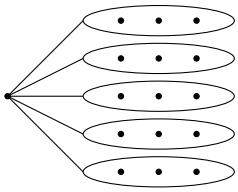
Definition 12.3. (Pairwise balanced GDD, PGDD)

A PGDD $(\mathbb{X}, \mathbb{B})$ of order v denoted by GD$(R, m; S, \lambda)$ is a (general) GDD of order v whose group sizes are in R and block sizes are in S. For example, the truncated T(r, 5, 1) is a GD$(\{r,\ r\}, 5; \{4,\ 5\}, 1)$ of order $4r + r_1$.

Lemma 12.4.

There exists a GD(3, 5; 4, 1). ($\{3\} \to 3,\ \{4\} \to 4$)

Proof. Since a 2-(16,4,1) design exists, a GD(3, 5; 4, 1) can be obtained by deleting one element from the design.

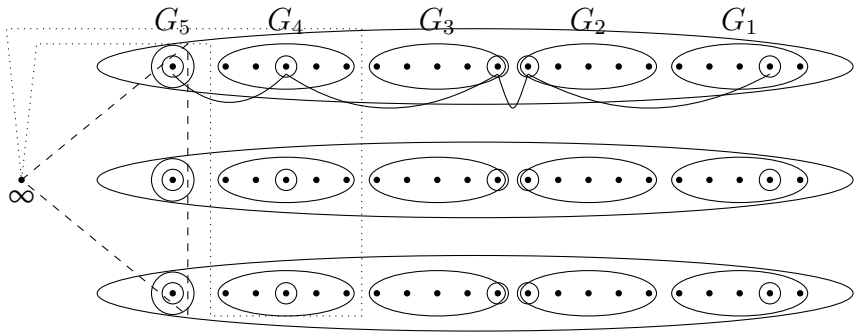


Here is an example to explain how can we constuct the design.

Example A 2-(64, 4, 1) design exists.

Proof. $64 = 3 \times 21 + 1$. (n in Lemma 12.1)

First, we use $r = 5$ and $r_1 = 1$ to obtain a GD($\{1, 5\}$, 5; 4, 1).



Construction $(\mathbb{X}, \mathbb{B})$

Step 1. ($\mathbb{B}_1$) Use $\{\infty\} \cup (G_i \times \{1, 2, 3\})$ to construct a 2-(4, 4, 1) design and 2-(16, 4, 1) design respectively.

Step 2. ($\mathbb{B}_2$) For each block $B \in$ GD($\{1, 5\}$, 5; 4, 1), construct a GD(3, 4; 4, 1) or GD(3, 5; 4, 1) depending on $B \times \{1, 2, 3\}$ and the size of B, $|B| = 4$ or 5. (See the figure above.)

Step 3. Let $\mathbb{X} = \{\infty\} \cup ((\bigcup_{i=1}^{5} G_i) \times \{1, 2, 3\})$, and $\mathbb{B} = \mathbb{B}_1 \cup \mathbb{B}_2$.

$|\mathbb{B}_1| = 1 + 4 \times 20 = 81.$

$|\mathbb{B}_2| = 5 \times 15 + 20 \times 9 = 255$ $\quad \Rightarrow \quad |\mathbb{B}| = 336.$

(∗) Any two elements occur together in a block. (Check!)

(∗∗) Small orders v s.t. a 2-$(v, 4, 1)$ design exists can be obtained by direct construction. "25" is the hardest one (?).

Theorem 12.5. A 2-$(v, 4, 1)$ design exists if and only if $v \equiv 1$ or 4 (mod 12).

Proof. ($\Rightarrow$) By Lemma 12.1.

($\Leftarrow$) We can construct all 2-$(v,4,1)$ designs recursively. Assume that small orders are constructed. Let $v = 3n + 1$ where $n \equiv 0$ or 1 (mod 4). By the above construction (or example), it suffices to write $n = 4r + r_1$ where $r > 0$, $r_1 \equiv 0$ or 1 (mod 4) and $3r+1$, $3r_1+1 \equiv 1$ or 4 (mod 12). (For example, if $n = 301$, then we can write $n = 4\times72+13$ where $r = 72$ and $r_1 = 13$. Since $3 \times 72 + 1 \equiv 1$ (mod 12) and $3 \times 13+1 \equiv 4$ (mod 12), we have a 2-(904, 4, 1) design.)

So, we have two cases to consider in general.

Case 1. $n \equiv 0$ (mod 4)

$n \equiv 4r + r_1$. If $r \equiv 0$ or 1 (mod 4) and $r_1 = 0$, the we are done. On the other hand, if $r_1 = 0$ and $r \equiv 2$ (mod 4), then let $n = 4(r - 1) + 4$. Further, if $r \equiv 3$ (mod 4), then let $n = 4(r - 2) + 8$. Hence, then GDD we use is of types $< r-1, r-1, r-1, r-1, 4 >$, and $< r-2, r-2, r-2, r-2, 8 >$ respectively.

Case 2. $n \equiv 1$ (mod 4)

Similarly, r_1 can be either 1 or 5 or 9 to make sure that the corresponding r satisfies $3r + 1 \equiv 1$ or 4 (mod 12). □

(∗) There are 16 non-isomorphic 2-(25, 4, 1) designs.
(See Handbook of Combinatorial Designs, p.12-13.)

(∗∗) 28 is obtained from $K_4|K_{9(3)}$. (Again, see Handbook.)

How about 2-$(v, k, 1)$ design where $k > 4$?

Observations

1. We need a GD$(R, m; k, 1)$ of certain order n first. $(m \geq k)$

2. A GD$(m', k; k, 1)$ and a GD$(m', k+1; k, 1)$ exists. ($m' = 3$ for $k = 4$.) $\Rightarrow v = 3n+1$.

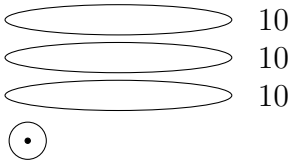
3. $\forall r \in R$, a 2-$(mr'+1, k, 1)$ design exists for each $r \in R$.

Review $k = 3$ (4^{th} construction!)

Consider $n \equiv 0$ or 1 (mod 3).

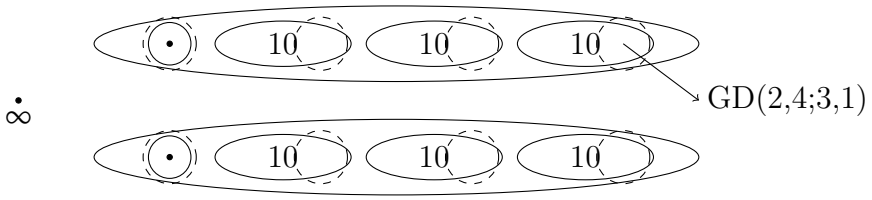
$R = \{3, 4\}$, $n = 3r + r_1$, $r_1 \equiv 0$ or 1 (mod 3). (T(r, 4, 1) exists.)

Example $n = 31$



GD(2, 3; 3, 1) and GD(2, 4; 3, 1) exist. ($m' = 2$)

2-(21, 3, 1) and 2-(3, 3, 1) exist.



($\cdot$) Here, r is chosen to satisfy $2r + 1 \equiv 1$ or 3 (mod 6), i.e., $r \equiv 0$ or 1 (mod 3).

($*$) If $\lambda > 1$, then we consider a 2-(v, k, λ) design as well.

In this case, the set of admissible v is larger than that for $\lambda = 1$ in general. For example, if $\lambda = 2$, $k = 3$, then we have $v \equiv 0$ or 1 (mod 3). We skip the details here.

13 Packing and Covering

Definition 13.1. (H-packing)

An H-packing of G is a collection of edge-disjoint subgraphs of G which are isomorphic to H. Let H be an H-packing of G. If $G \setminus \cup_{H \in \mathbb{H}} E(H)$ contains no subgraph which is isomorphic to H, then $\mathbb{H}$ is a maximal H-packing. Furthermore, if $\mathbb{H}$ contains the maximum number of copies of H, then $\mathbb{H}$ is a maximum H-packing.

For convenience, let $L = G \setminus \cup_{H \in \mathbb{H}} E(H)$. L is called the leave of the H-packing $\mathbb{H}$ with respect to G.

$(\cdot)$ It is interesting to know "the maximum packing".

Theorem 13.2.

The maximum packing of K_v with K_3's is obtained by using the following table where the minimum leaves are listed.

v	0	1	2	3	4	5	(mod 6)
L	F	ϕ	F	ϕ	T	C_4	F is 1-factor and T is tripole.

Proof.

Case 1: $v \equiv 1$ or 3 (mod 6). It follows by the existence of an $STS(v)$.

Case 2: $v \equiv 5$ (mod 6). It follows by the existence of a 2-$(v, \{3, 5^*\}, 1)$ design.

Case 3: $v \equiv 0$ or 2 (mod 6). By deleting a vertex from K_{v+1} we obtain the packings.

Case 4: $v \equiv 4$ (mod 6). By deleting a vertex from K_{v+1} which is in K_5 of the design in Case 2, we have the conclusion.

Note that the leaves we obtain are minimum, therefore the packings are maximum respectively. □

Open problem For which leaves L, $K_3 \mid K_v - L$?

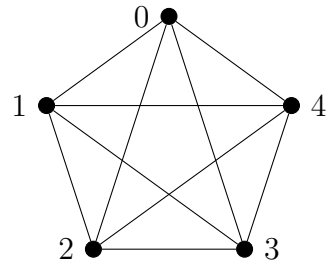
$(*)$ Clearly, $K_v - L$ must be 3-sufficient, i.e. each vertex is of even degree and $3 \mid \|K_v - L\|$.

Covering

Definition 13.3. (H-covering)

An H-covering of G is a collection $\mathbb{H}$ of edge-disjoint subgraphs of G which are isomorphic to H such that each edge of G is covered by at least one member of $\mathbb{H}$. Then the collection $\mathbb{H}$ is a minimum covering of G if $\Sigma_{H\in\mathbb{H}}\|H\| - \|G\|$ is minimum.

e.g.



$\{012, 034, 134, 234\}$ is a minimum covering of K_5 with K_3's.

(·) The set of extra edges induces a "padding" of the covering. The above example shows that  is the padding.

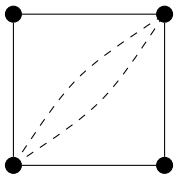
(·) The padding obtained is a minimum covering is called a minimum padding.

Theorem 13.4.

The minimum covering of K_v by using copies of K_3 is obtained as in the following table.

v	0	1	2	3	4	5	(mod 6)
P	F	ϕ	T	ϕ	T	D_2	D_2 is 

Proof. For $v \equiv 1$ or 3 (mod 6), if follows from the existence of an $STS(v)$. As to $v \equiv 5$ (mod 6), since $L = C_3$ provides a maximum packing, it suffices to cover C_4 by using two extra K_3's such that D_2 is the padding.



Now, we consider $v \equiv 0 \pmod 6$. First, we find the maximum packing of K_{v-2} with leave a tripole T. So, we shall add two verices u and v to cover $T \cup F'$ where F' is a 1-factor of K_v with an extra edge uv, see the following figure.

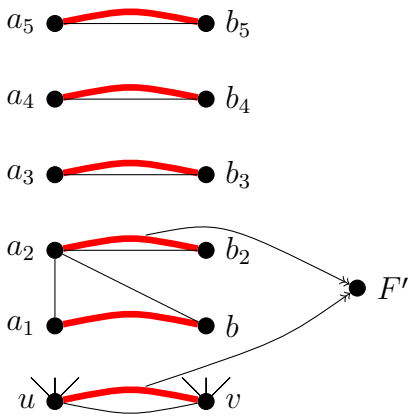
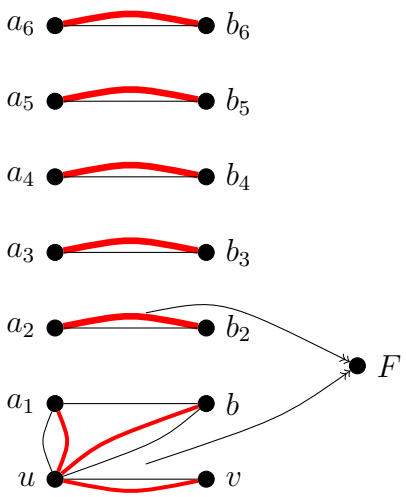


Figure. Use $v = 12$ for example

(Black edges are in leave, red edges are added)

It is easy to check that there are 33 edges to be packed by using K_3's. The following K_3's are in the packing. $a_1a_2b_1, a_1uv, b_1uv, ua_2b_2, va_2b_2, ua_3b_3$,
$va_3b_3, ua_4b_4, va_4b_4, ua_5b_5, va_5b_5$. Note that $F' - uv$ is the minimum padding.

Finally, let $v \equiv 2$ or $4 \pmod 6$. Since there two cases are similar, we consider $v \equiv 2 \pmod 6$ and use $v = 12$ for example to explain the idea of proof. Again we have the maximum packing of $K_{v-2} \cong K_{12}$. Therefore, the minimum leave is a 1-factor, see the following figure for explanation. Let T (red edges) be the padding we plan to add.



K_3's: $a_1uv, b_1uv, ua_1b_1, ua_2b_2, va_2b_2, \cdots, ua_6b_6, va_6b_6$.

□

(·) The reason why these paddings are minimum comes from the degree and size conditions.

It is important to know that if K_v has a maximum K_k-packing $\mathbb{H}$ with m members in $\mathbb{H}$, then almost all pairs are covered by using K_k's except these pairs in the leave. Clearly, for these orders in which no 2-$(v, k, 1)$ designs exist, this is the best job we can do.

Moreover, as packing is concerned, a graph G can be packed with not only one subgraph. For example, we may use a path of length s and a cycle of length t to pack K_v. Hence, we shall have a $\{P_{s+1}, C_t\}$-packing of K_v. Of course, K_v can be replaced by other graphs, say $K_{m(n)}$ or a general graph.

14 t-design

Definition 14.1. A t-design, t-(v,k,λ) design, is an $(\mathbb{X},\mathbb{B})$ such that $|\mathbb{X}| = v$, $\forall B \in \mathbb{B}$, $|B| = k$, and for each t-subset of $\mathbb{X}$, it occurs exactly λ times in the blocks of $\mathbb{B}$.

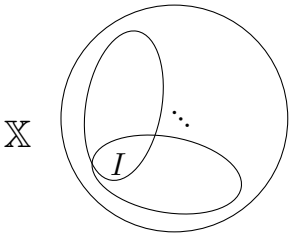
When $t \geq 3$, then finding a good t-design is getting more complicate especially when the block size is also larger. The followings are some basic properties of t-designs.

- If $(\mathbb{X},\mathbb{B})$ is a t-(v,k,λ) design, then

  (a) $\lambda\binom{v}{t}/\binom{k}{t}$ is an integer,

  (b) for each $0 \leq i \leq t$, the collection of all blocks $\mathbb{B}_i$ containing a given i-subset of $\mathbb{X}$ is exactly $\lambda\binom{v-i}{t-i}/\binom{k-i}{t-i}$, and

  (c) if I is an i-subset with $i \leq t$, then the collection of blocks $\mathbb{B}_i = \{B\backslash I | B \in \mathbb{B}\}$ with $\mathbb{X}_i = \mathbb{X} - I$ is a $(t-i)$-$(v-i,k-i,\lambda)$ design.



- Let $k \geq t \geq 2$. Then, the collection of all k-subsets of $\mathbb{X} = \mathbb{Z}_v$ is in fact a t-design t-(v,k,λ) design where $\lambda = \binom{v-t}{k-t}$ if $k > t$ and $\lambda = 1$ if $k = t$.

- If $k = 3$ and $t = 2$, then $\binom{\mathbb{Z}_v}{3}$ forms a 2-$(v,3,\lambda)$ design where $\lambda = v-2$. (If $k = 4$ and $t = 2$, then $\binom{\mathbb{Z}_v}{4}$ is a 2-$(v,4,\lambda)$ design with $\lambda = \binom{v-2}{2}$.)

- In case of $k = 3$, if $\binom{\mathbb{Z}_v}{3}$ can be partitioned into $v-2$ disjoint STS(v)'s, then we have a large set of Steiner triple systems.

$(*)$ You may try the case when $v = 7$ and $k = 3$.

Theorem 14.2. (Lu, Jia-Xi) 1935-1983

A large set of STS(v)'s exists except for some small cases.

(Reference: Lu Jia-Xi, On large sets of disjoint Steiner triple systems I, J. Combinatorial Theory 34A (1983), 140-146.)

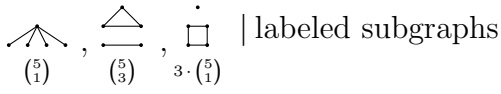
Definition 14.3. (Steiner systems)

In a t-design $(\mathbb{X}, \mathbb{B})$, if $k = t+1$ and $\lambda = 1$, then we have a Steiner t-design of order $|\mathbb{X}|$. A Steiner triple system of order v is a 2-$(v,3,1)$ design and a Steiner guadruple system of order v is a 3-$(v,4,1)$ design or S(t,k,v) in short where $t = k-1$.

- **Small example** $t = 3$ and $k = 4$

  Let $\mathbb{X} = \mathbb{Z}_2^4$ and $\mathbb{B}\left\{\{\vec{w},\vec{x},\vec{y},\vec{z}\} \mid \vec{w},\vec{x},\vec{y},\vec{z} \in \mathbb{Z}_2^4,\ \vec{w}+\vec{x}+\vec{y}+\vec{z} = \vec{0}\right\}$.

  Note that $\vec{x},\vec{y},\vec{z}$ and $\vec{w}$ are distinct vectors. Then, $(\mathbb{Z}_2^4, \mathbb{B})$ is an S(3,4,16). It is also true for an S$(3,4,2^m)$ where $m \in \mathbb{N}$.

- Let $\mathbb{X} = E(K_5)$ and $\mathbb{B} = \{$  $\mid$ labeled subgraphs of $K_5\}$.

  Then, $(\mathbb{X}, \mathbb{B})$ is an S(3,4,10).

- How about $t = 3$ and v in general?

- $v \equiv 2$ or 4 (mod 6). (Let $(\mathbb{X}, \mathbb{B})$ be an S(3,4,v).) Let $x_0 \in \mathbb{X}$ $(\mathbb{X}' = \mathbb{X}\backslash\{x_0\})$ and $\mathbb{B}' = \{B\backslash\{x_0\} | B \in \mathbb{B}\}$. Then, $(\mathbb{X}', \mathbb{B}')$ is an STS(v-1). This implies that $|\mathbb{X}'| = v-1 \equiv 1$ or 3 (mod 6).

Theorem 14.4. (H. Hanani, 1960)

An S(3,4,v) exists if and only if $v \equiv 2$ or 4 (mod 6).

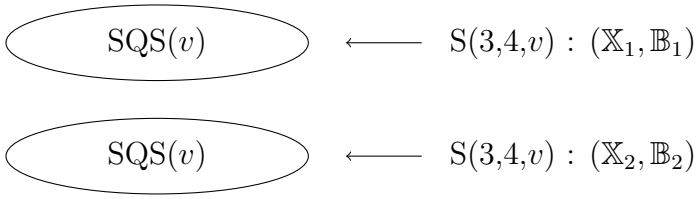
Proof. It takes a let of effort in proving the sufficient part.

Doubling Construction

Construction 1. An $S(3,4,2v)$ exists if an S(3,4,v) exists.

Proof.

(a) (Method 1)



Let $K_{\mathbb{X}_i}$ denote the complete graph defined on $\mathbb{X}_i,\ i = 1, 2$. Since $|\mathbb{X}_i|$ is even, $K_{\mathbb{X}_i}$ can be decomposed into 1-factors, there are v-1 of them, called $F_1, F_2, \cdots, F_{v-1}$ and $G_1, G_2, \cdots, G_{v-1}$ for $i = 1, 2$ respectively. Now, we use F_j and $G_j,\ j = 1, 2, \cdots, v-1$ to defind $(\frac{v}{2})^2$ quadruples by the following way :

$$\left.\begin{array}{l} F_j = \{\{a_i, b_i\} \,|\, i = 1, 2, \cdots, \frac{v}{2}\} \\ G_j = \{\{c_j, d_j\} \,|\, j = 1, 2, \cdots, \frac{v}{2}\} \end{array}\right\} \Rightarrow\ \{a_i, b_i, c_j, d_j\} \in \mathbb{B}.$$

Combining the above blocks with $\mathbb{B}_1$ and $\mathbb{B}_2$, we have an S(3,4,2v).

$(*)$ This SQS($2v$) contains two disjoint sub-design SQS(v) (or SQS($2v$)).

(b) (Method 2) Let $Y' = \{y' \,|\, y \in Y\}$ and $\mathbb{X} = Y \cup Y'$. Let $(Y, \mathbb{C})$ be an SQS(v). Define $\mathbb{B}$.

(1) $\forall \{x, y, z, w\} \in \mathbb{C}$, let $\{x, y, z, w'\}, \{x, y, z', w\}, \{x, y', z, w\}$, $\{x', y, z, w\}, \{x', y', z', w\}, \{x', y', z, w'\}, \{x', y, z', w'\}$ and $\{x, y', z', w'\}$ be in $\mathbb{B}$.

(2) For any two elements $\{x, y\} \subseteq Y$, let $\{x, y, x', y'\} \in \mathbb{B}$. Combining (1),(2), we have an SQS($2v$) = $(\mathbb{X}, \mathbb{B})$.

It is a routine matter to check $(\mathbb{X}, \mathbb{B})$ is indeed an SQS($2v$) for both constructions : (a) and (b).

The above doubling construction can only handle the cases $v \equiv 4$ or $8 \pmod{12}$. For the other cases, it takes more effort. (We omit the details here and present $v \to 3v-2$ construction.)

Let $q(v) = \frac{v(v-1)(v-2)}{24}$, $p(v') = \frac{v'(v'-1)}{6}$ and $q'(v) = q(v) - p(v-1)$.

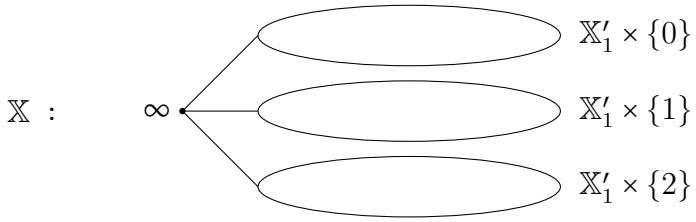
$(\cdot)$ If $v \equiv 2$ or $4 \pmod{6}$, then $p(v-1) = \frac{(v-1)(v-2)}{6}$.

Consider $u \equiv 4$ or $10 \pmod{18}$.

$u = 3v-2$ where $v \equiv 2$ or $4 \pmod{6}$. (Example : if $v = 8$, then $u = 22$.)

Construction of SQS(u)

Let $(\mathbb{X}_1, \mathbb{B}_1)$ be an SQS(v) such that $\infty \in \mathbb{X}_1$. Let $\mathbb{X} = \{\infty\} \cup \mathbb{X}_1' \times \mathbb{Z}_3$ where $\mathbb{X}_1' = \mathbb{X}_1 \backslash \{\infty\}$. So,



Quadruples ($\mathbb{B}$)

1. $\forall \{x,y,z,w\} \subseteq \mathbb{X}_1'$ and $\{x,y,z,w\} \in \mathbb{B}_1$, let $\{(x,a_1),(y,a_2),(z,a_3),(w,a_4)\} \in \mathbb{B}$ where $a_1 + a_2 + a_3 + a_4 \equiv 0 \pmod{3}$.
   $((a_1,a_2,a_3,a_4) \in \{(0,0,0,0),(0,1,1,1),(1,0,1,1),(1,1,0,1),(1,1,1,0),$
   $(0,2,2,2),(2,0,2,2),(2,2,0,2),(2,2,2,0)$, and 18 others$\}$.)
   $(\cdot)$ Type 1 quadruples : $27 \times q'(v)$ quadruples. $\left(27 \cdot \left(\frac{v(v-1)(v-2)}{24} - \frac{(v-1)(v-2)}{6}\right)\right)$

2. For $\{\infty,u,v,w\} \in \mathbb{B}_1$, define the following quadruples and let them in $\mathbb{B}$:
   $\{\infty,(u,b_1),(v,b_2),(w,b_3)\} \in \mathbb{B}$ where $b_1 + b_2 + b_3 \equiv 0 \pmod{3}$.
   $((b_1,b_2,b_3) \in \{(0,0,0),\ (1,1,1),\ (2,2,2),\ (0,1,2),\ (0,2,1),\ (1,0,2),$
   $(1,2,0),\ (2,0,1),\ (2,1,0)\}$.)
   We have $9 \times p(v-1)$ such quadruples. $\left(\frac{9(v-1)(v-2)}{6}\right)$.

3. Continue from 2.

$\{(u,i),(v,i),(w,i+1),(w,i+2)\},\ i \in \mathbb{Z}_3.$

$\binom{3}{2} \cdot 3$ $\qquad 9 \cdot p(v-1)$ quadruples.

4. $\forall$ pair (α,β) in $\mathbb{X}_1'$, let

   $\{(\alpha,i),(\beta,i),(\alpha,i+1),(\beta,i+1)\} \in \mathbb{B}$. $\left(3 \cdot \binom{v-1}{2}\right.$ quadruples$\left.\right)$

5. $\forall\, \gamma \in \mathbb{X}_1'$, let

   $\{\infty,(\gamma,0),(\gamma,1),(\gamma,2)\} \in \mathbb{B}$. $(v-1$ quadruples$)$

In total, we have $27 \cdot \left(\frac{v(v-1)(v-2)}{24} - \frac{(v-1)(v-2)}{6}\right) + 9 \cdot \frac{(v-1)(v-2)}{6} + 9 \cdot \frac{(v-1)(v-2)}{6} + 9 \cdot \frac{(v-1)(v-2)}{6} + (v-1) = \frac{27}{24}v(v-1)(v-2) + (v-1) = \frac{(3v-2)(3v-3)(3v-4)}{24}$.

How about the other cases ?

Conjecture $v \to 2v+6$ constuction

For each SQS(v) $(\mathbb{X}_1,\mathbb{B}_1)$, there exists an SQS($2v+6$) which contain $(\mathbb{X}_1,\mathbb{B}_1)$ as as subsystem.

Hanani's Construction

1. $n \equiv 4$ or $8 \pmod{12}$

   $v \to 2v$;

2. $n \equiv 4$ or $10 \pmod{18}$

   $v \to 3v-2$;

3. $n \equiv 34$ or $8 \pmod{36}$

   $v \to 3v+4$ where $v \equiv 10 \pmod{12}$;

4. $n \equiv 26$ or $8 \pmod{36}$

   $v \to 3v+2$ where $v \equiv 8 \pmod{12}$;

5. $n \equiv 2$ or $10 \pmod{24}$

   $v \to 4v-6$ where $v \equiv 2$ or $4 \pmod{6}$; and

6. $n \equiv 14$ or $38 \pmod{72}$

   $v \to 12v - 10$ where $v \equiv 2$ or $4 \pmod 6$.

($*$) If we have $v \to 2v$ and $v \to 2v + 6$ constructions, then the theorem about the existence of SQS(v)'s is proved.

Proof. Consider $v \equiv 2$ or 4 or 8 or $10 \pmod{12}$. Clearly, if $v \equiv 4$ or $8 \pmod{12}$, then by $v \to 2v$, we can construct such a system. On the other hand, if $v \equiv 2$ or $10 \pmod{12}$, let $v = 12k + 2$ or $12k + 10$ respectively. By direct counting, $12k + 2 = 2(6k - 2) + 6$ and $12k + 10 = 2(6k + 2) + 6$. Hence, the construction $v \to 2v + 6$ works. □

The best known construction besides $v \to 2v$ on SQS(v) is the following.

Theorem 14.5. (Hartman) (Tripling Construction !)

If an SQS(v) contains a subsystem SQS(u), then there exists an SQS($3v - 2u$) which contains the above SQS(v)

Note that we can also use this theorem to prove the cases $v \equiv 2$ or $10 \pmod{12}$ except some small cases. (?)

$v \equiv 2$ or $10 \pmod{12}$

$\Rightarrow v \equiv 2, 10, 14, 22, 26, 34 \pmod{36}$

$36k + 2 = 3(12k + 2) - 4$	$u = 2$	SQS(2) is a trivial system
$36k + 10 = 3(12k + 4) - 2$	$u = 1$	(one element)
$36k + 14 = 3(12k + 10) - 16$	$u = 8$	
$36k + 22 = 3(12k + 14) - 20$	$u = 10$	
$36k + 26 = 3(12k + 14) - 16$	$u = 2$	
$36k + 34 = 3(12k + 14) - 8$	$u = 4$	

15 Hadamard matrices

Definition 15.1. ($\mathcal{H}$-matrix)

A square $n \times n$ matrix H is called an Hadamard matrix (an $\mathcal{H}$-matrix) of order n if all the entries of H are ± 1 and $HH^T = nI_n$ where I_n is the identity matrix of order n.

Examples

$$\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \text{ or } \begin{bmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

We called the second matrix has standard form since the first row and column of second matrix are all 1's.

Fact 1. If H is an $\mathcal{H}$-matrix, then H^T is also an $\mathcal{H}$-matrix.

Definition 15.2. (Generalized permutation matrices, G.P.M.)

An $n \times n$ generalized permutation matrix is an $n \times n$ matrix in which each row (and each column) contains exactly one non-zero entry.

Furthermore, if all non-zero entries are either +1 or −1, then we have a monomial permutation matrix (M.P.M.). For example,

$$\begin{bmatrix} 0 & 2 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & \sqrt{3} \\ 0 & 0 & 7 & 0 \end{bmatrix} \text{ is a G.P.M., and } \begin{bmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \text{ is an M.P.M.}$$

(·) We may permute the rows and columns of a G.P.M. to obtain a diagonal (invertible) matrix.

Fact 2 Let A and B be monomial permutation matrices. Then, H is an $\mathcal{H}$-matrix if and only if AHB is an $\mathcal{H}$-matrix.

Proof. Note that if A is an $n \times n$ M.P.M., then AA^T is a permutation matrix, I_n, i.e. $AA^T = I_n$ and $A^T = A^{-1}$. (A^T is also an M.P.M.)

($\Rightarrow$) $(AHB)(AHB)^T = AHBB^TH^TA^T = AHH^TA^T = nI_n$.

($\Leftarrow$) Since AHB is an $\mathcal{H}$-matrix, $A^{-1}(AHB)B^{-1}$ is an $\mathcal{H}$-matrix by ($\Rightarrow$). Hence, H is an $\mathcal{H}$-matrix. □

Definition 15.3. ($\mathcal{H}$-equivalent)

Two $\mathcal{H}$-matrices H_1 and H_2 are $\mathcal{H}$-equivalent if there exist generalized (monomial) permutation matrices A and B s.t. $H_2 = AH_1B$.

Fact 3 Any $\mathcal{H}$-matrix is $\mathcal{H}$-equivalent to an $\mathcal{H}$-matrix with every entry in the first row and first column equal to +1.

Proof. Let $I_n(i)$ denote the generalized permutation matrix obtained from I_n by replacing the (i,i) entry with -1. Then, by applying $I_n(i)$ we can change the sign of the ith row and ith column of H resp. ($I_n(i) \cdot H$ or $H \cdot I_n(i)$) □

Fact 4 (N.C. of the existence of an $\mathcal{H}$-matrix)

If H is an $\mathcal{H}$-matrix of order n, then $n = 1$ or 2, or $n \equiv 0 \pmod 4$.

Proof. For $n \geq 4$. W.L.O.G. let H be a stand and $\mathcal{H}$-matrix, i.e. all +1's in the first row and first column. By considering the orthogonality of the first three rows, we conclude the proof. □

Conjecture

$\forall n \equiv 0 \pmod 4$, there exists an $\mathcal{H}$-matrix of order n. (Many results have been obtained, but not settled in general.)

Fact 5 (Doubling construction)

If H is an $\mathcal{H}$-matrix of order n, then $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}$ is also an $\mathcal{H}$-matrix which is of

order $2n$.

Proof. $\begin{pmatrix} H & H \\ H & -H \end{pmatrix}\begin{pmatrix} H & H \\ H & -H \end{pmatrix}^T = \begin{pmatrix} H & H \\ H & -H \end{pmatrix}\begin{pmatrix} H^T & H^T \\ H^T & (-H)^T \end{pmatrix} =$

$\begin{pmatrix} HH^T + HH^T & HH^T - HH^T \\ HH^T - HH^T & HH^T + HH^T \end{pmatrix} = \begin{pmatrix} 2I_n & 0 \\ 0 & 2I_n \end{pmatrix} = 2I_{2n}.$ □

Fact 6 For each $n = 2^t$, there exists an $\mathcal{H}$-matrix of order n. (By Fact 5)

Example

Let $S_i = [s_{i,j}]$ be a matrix. We use $a \otimes S = [a \cdot s_{i,j}]$.

$$S = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (-1) \otimes S = \begin{bmatrix} -1 & -1 & -1 & -1 \\ -1 & 1 & -1 & 1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

Fact 7 If $M = [m_{i,j}]_{m\times m}$ and $S = [s_{i,j}]_{s\times s}$ are $\mathcal{H}$-matrices, then $M \otimes S$ is also an $\mathcal{H}$-matrix where

$$M \otimes S = \begin{bmatrix} m_{1,1} \otimes S & m_{1,2} \otimes S & \cdots & m_{1,m} \otimes S \\ & & \cdots & \\ m_{m,1} \otimes S & m_{m,2} \otimes S & \cdots & m_{m,m} \otimes S \end{bmatrix}.$$

Clearly, $M \otimes S$ is of order $m \cdot s$.

Proof. Let $H = (M \otimes S) \cdot (M \otimes S)^T$. Then, $H(i,j)$ is equal to $\Sigma_{k=1}^{m}(m_{i,k} \otimes S) \cdot (m_{j,k} \otimes S) = \Sigma_{k=1}^{m} m_{i,k} \cdot m_{j,k} \cdot sI_s = sI_s$ iff $i = j$ □

Fact 8 There exists an $\mathcal{H}$-matrix of order 12 and therefore there exist $\mathcal{H}$-matrices of order 3×2^t where $t \geq 2$.

Proof. (Williamson's method)

Let

$$H = \begin{bmatrix} A & B & C & D \\ -B & A & -D & C \\ -C & D & A & -B \\ -D & -C & B & A \end{bmatrix}$$

where $A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ and $B = C = D = \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & 1 \end{bmatrix}$. Now, we have $A^2 = \begin{bmatrix} 3 & 3 & 3 \\ 3 & 3 & 3 \\ 3 & 3 & 3 \end{bmatrix}$ and $B^2 = C^2 = D^2 = \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix}$. Moreover, $AB = BA, AC = CA, AD = DA$, in fact, all of them are the same, $\begin{bmatrix} -1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & -1 \end{bmatrix}$.

Again, by using the multiplication of block form, we have

$$H \cdot H^T = \begin{bmatrix} A^2 + B^2 + C^2 + D^2 & & \mathbf{0} \\ & \ddots & \\ \mathbf{0} & & A^2 + B^2 + C^2 + D^2 \end{bmatrix} = 12I_{12}.$$

□

Fact 9 If there exists an $\mathcal{H}$-matrix of order $4k$, then there exists a 2-$(4k-1, 2k-1, k-1)$ design.

Proof. Let H be an $\mathcal{H}$-matrix of standard form. Now, by deleting the first row and first column, and replace all (-1)'s with 0's, we obtain a $(0,1)$-matrix H' of order $4k-1$. (For example, $k = 2$ we have

$$H = \left[\begin{array}{c|ccccccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{array}\right] \Rightarrow \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \end{array} \begin{array}{c} \begin{array}{ccccccc} B_1 & B_2 & B_3 & B_4 & B_5 & B_6 & B_7 \end{array} \\ \left[\begin{array}{ccccccc} 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{array}\right] \end{array}$$

.

With idea of support by assigning row indices as $\mathbb{Z}_{4k-1}$ we have $4k-1$ blocks. So, in the example of $k = 2$, the blocks are $123, 034, 236, 012,$
$146, 056, 245.$

As to the design $(\mathbb{X}, \mathbb{B})$, we conclude that $|\mathbb{X}| = |\mathbb{B}| = 4k-1$, and for each $B \in \mathbb{B}$, $|B| = 2k-1$, since we have $2k-1$ 1's left.

For the λ of the design $(\mathbb{X}, \mathbb{B})$, we observe that in every two rows of H', they have exactly $k-1$ common 1's in order to satisfy the orthogonality in H.

$$\begin{array}{cccc} & \overbrace{\cdots 1 \cdots}^{2k-1} & \overbrace{\cdots -1 \cdots}^{2k} & 1+s=t \\ 1 & & & 1+s+t=2k \\ 1 & \underbrace{s}_{1} \quad \underbrace{}_{-1} & \underbrace{t}_{1} \quad \underbrace{}_{-1} & 2+2s=2k \\ & & & s=k-1 \end{array}$$

Hence, we have a 2-$(4k-1, 2k-1, k-1)$ design, in fact, it is a symmetric design. That is, a symmetric design exists (with certain parameters) if an $\mathcal{H}$-matrix of certain order exists. □

On the existence of circulant Hadamard matrices

As mentioned above, an Hadamard matrix of order n is a (± 1)-matrix such that any two distinct row vectors of length n are orthogonal, i.e., their inner product is "0".

Now, if we impose an extra condition that all the rows of the matrix can be obtained by cyclic shift of the first row, then we have a "circulant" Hadamard matrix. For example,

$$\begin{bmatrix} -1 & +1 & +1 & +1 \\ +1 & -1 & +1 & +1 \\ +1 & +1 & -1 & +1 \\ +1 & +1 & +1 & -1 \end{bmatrix} \Rightarrow \begin{bmatrix} - & + & + & + \\ + & - & + & + \\ + & + & - & + \\ + & + & + & - \end{bmatrix} \quad \text{(short form)}$$

Problem Are there circulant Hadamard matrices of order larger than 4 ?

(•) Let $\vec{a} = (a_0, a_1, \cdots, a_{n-1})$. The cyclic shift of $\vec{a}$ is defined as $\alpha^i(\vec{a}) = (a_{-i}, a_{1-i}, \cdots, a_{n-1-i})$ for $i = 1, 2, \cdots, n-1$, where the indices are modulo n. Hence,

$$\alpha(\vec{a}) = (a_{n-1}, a_0, a_1, \cdots, a_{n-2}) \text{ and}$$
$$\alpha^2(\vec{a}) = (a_{n-2}, a_{n-1}, a_0, a_1, \cdots, a_{n-3}).$$

(•) If A is a circulant $\mathcal{H}$-matrix, then its rows are denoted by vectors $A_0, A_1, \cdots, A_{n-1}$, such that $A_i = \alpha^i(A_0)$.

(•) For fixed $k \in \{1, 2, \cdots, n-1\}$, let

$$x_k = |\{(a_i, a_{i-k}) = (+1, +1)\}|,$$
$$y_k = |\{(a_i, a_{i-k}) = (+1, -1)\}|,$$
$$z_k = |\{(a_i, a_{i-k}) = (-1, +1)\}|, \text{ and}$$
$$w_k = |\{(a_i, a_{i-k}) = (-1, -1)\}|.$$

(∗) Since A is a circulant, x_k, y_k, z_k and w_k are independent to $i \in \mathbb{Z}_n$.

Now, we are ready to prove the following theorem.

Theorem 15.4. If A is a circulant $\mathcal{H}$-matrix of order n, then $n = 4t^2$ for some $t \in \mathbb{N}$.

Proof. If A is an H-matrix, A_i is orthogonal to A_j for $j \neq i$.

Therefore, we may assume that

$$A_i = (\overbrace{+ + \cdots +}^{\frac{n}{2}} \overbrace{- - \cdots -}^{\frac{n}{2}}) \quad \text{and} \quad A_{i+k} = (\overbrace{+ + \cdots +}^{\frac{n}{4}} \overbrace{- - \cdots -}^{\frac{n}{4}} \overbrace{+ + \cdots +}^{\frac{n}{4}} \overbrace{- - \cdots -}^{\frac{n}{4}})$$

(for convenience to understand).

This implies that

(1) $x_k + y_k + z_k + w_k = n$

(2) $x_k + w_k = y_k + z_k$, and

(3) If p is the number of (+1)'s and q is the number of (-1)'s, then $p+q = n$, $x_k + y_k = x_k + z_k = p$.

Hence, $y_k = z_k$ and $n = 4\,y_k \equiv 0 \pmod 4$. So, n is even.

Consider A_0 and $A_{\frac{n}{2}}$:

$$\begin{pmatrix} a_0 & a_1 & \cdots & a_{\frac{n}{2}} & \cdots & a_{n-1} \\ a_{\frac{n}{2}} & a_{\frac{n}{2}+1} & \cdots & a_0 & \cdots & a_{\frac{n}{2}-1} \end{pmatrix}.$$

If $(a_i, a_{i+\frac{n}{2}}) = (\delta, \delta)$ where $\delta = +1$ or -1, so is $(a_{i+\frac{n}{2}}, a_i)$. Thus, both x_k and w_k are even. Moreover, $y_k + z_k = \frac{n}{2}$ and $\sum_{k=1}^{n-1}(y_k + z_k) = \frac{n(n-1)}{2}$. The second equality gives the total number of $(+1,-1)$ or $(-1,+1)$ pairs for one row to pair with the other $n-1$ rows. Equivalently, the number of such pairs can also be equal to $pq + qp$ by counting all $(+1,-1)$ or $(-1,+1)$ pairs. Then, $pq + qp = 2p(n-p) = \frac{1}{2}n(n-1)$. As a consequence, $(2p-n)^2 = n$, i.e., $n = 4(p - \frac{n}{2})^2$. This fact also implies that no circulant $\mathcal{H}$-matrices exist when $p = q$ when $n > 4$. □

From the above observation, we can conclude that if a circulant $\mathcal{H}$-matrix exists, then in each row (resp. column) the number of (+1)'s, $p = \frac{1}{2}(n + \sqrt{n})$ and the number of (-1)'s, $q = \frac{1}{2}(n - \sqrt{n})$. So far, except for $n = 4$, no other circulant $\mathcal{H}$-matrices have been found. As a matter of fact, if $n = 2^{2a+1}$,$a \geq 1$, no such matrices exist (by using

Algebra), see the M.S. thesis by Hui-Chung Ko, "On the construction of circulant **near** Hadamard matrices", NCTU, 2020.

Definition 15.5. (CPHM)

A circulant partial $\mathcal{H}$-matrix of order n, A, with m rows is an $m \times n$ (± 1)-matrix such that its m rows are $A_0, A_1, \cdots, A_{m-1}$ where $A_i = \alpha^i(A_0)$ and $AA^T = nI_m$.

e.g., $n = 8$ and $m = 3$

$$\begin{bmatrix} + & + & + & - & + & - & - & - \\ - & + & + & + & - & + & - & - \\ - & - & + & + & + & - & + & - \end{bmatrix}$$

Figure 1.

Note that we can keep shifting rows to obtain a circulant matrix A_D of order 8, but $A_D A_D^T \neq 8I_8$, i.e., A_D is not an $\mathcal{H}$-matrix. Again, by observation, we can use any three consecutive rows to obtain a PCHM of order 8 with $m = 3$.

Definition 15.6. (Circulant near $\mathcal{H}$-matrix)(CNHM)

A **circulant** matrix A of order n with entries ± 1 is said to be a circulant near $\mathcal{H}$-matrix if it contains the maximum number of zeros in each rows of AA^T, we use α_n to denote this number.

Clearly, the above example shows that $\alpha_8 \geq 3$. In order to maximize α_n, we have to choose the first row, an n-vector, properly. Now, let $A_0 = (a_0, a_1, \cdots, a_{n-1})$ where $a_i \in \{+1, -1\}$, $i \in \mathbb{Z}_n$. By letting "-1" be replace by "0", then we obtain a $(0,1)$-vector, D_0. Therefore, we can represent A_0 by a set $S_0 = \{i \mid a_i = 1,\ i \in \mathbb{Z}_n\}$, i.e., $S_0 = \text{supp}(D_0)$. For example, $(+,+,+,-,+,-,-,-)$ can be represented by $\{0,1,2,4\}$.

The set of differences

(•) Differences are defined on "abelian groups" in general.

(•) For convenience, we consider $< \mathbb{Z}_v, + >$.

(•) Therefore, $\forall\ a, b \in \mathbb{Z}_v,\ a - b = a + b^{-1} \pmod{v}$.

(∗) Let $D \subseteq \mathbb{Z}_v$ and $|D| = k$. Then, there are k^2 differences including k of them are 0's and the others are in pairs, i.e., if d is a difference obtained from D, then $v - d$ is also a difference. Sometimes, we use $\pm d$ to denote the differences.

Definition 15.7.

A (v, k, λ)-difference set is a set $D = \{d_1, d_2, \cdots, d_k\}$ of distinct elements of $\mathbb{Z}_v$ s.t. each difference d appears exactly λ times in $\Delta_D = \{d = d_i - d_j \pmod{v} \mid i \neq j\}$. (The difference "0" is not included here.)

We can generalize the above notion in two ways.

(1) Instead of using D, we use $\mathbb{D} = \{D_1, D_2, \cdots, D_n\}$. A generalize (v, k, λ)-difference collection satisfies :
in $\bigcup_{i=1}^{n} \Delta_{D_i}$, each difference d occurs exactly λ times. (See cyclic construction of STS(v) for example.) $\mathbb{D}$ is known as a set of base-blocks.

(2) The differences appear differently in "times". For example, if $D = \{1, 2, 3, 5\}$, then $\Delta_D = \{1, 1, 2, 2, 3, 4, 4, 5, 6, 6, 7, 7\}$. A generalized
$(v, k; \lambda_0, \lambda_1, \cdots, \lambda_{v-1})$-difference set (GDS) satisfies the difference d appears exactly λ_d times, $d \in \mathbb{Z}_v$. We use Δ to denote $\Delta_D \cup \{0, 0, \cdots, 0\}$ (multi-set of v 0's). For convenience, we use (v, k, Λ) - difference set in short where $\Lambda = \{\lambda_0, \lambda_1, \cdots, \lambda_{v-1}\} = \{\lambda_i \mid i \in \mathbb{Z}_v\}$.

Theorem 15.8. If there exists a $(4t^2, 2t^2 + t, t^2 + t)$ - difference set D, then we have a circulant $\mathcal{H}$-matrix of order $4t^2$.

Proof. If suffices to show that any two rows of the following matrix A_D are orthogonal.

Let $A_D^{(0)} = (a_0, a_1, \cdots, a_{4t^2-1})$ where $a_i = +1$ if $i \in D$ and -1 otherwise. Then, A_D is a $4t^2 \times 4t^2$ matrix corresponding to D by shifting $A_D^{(0)}$ $4t^2 - 1$ times.

Example

$$A_D = \begin{bmatrix} a_0 & a_1 & \cdots & \cdots & a_{4t^2-1} \\ a_{4t^2-1} & a_0 & a_1 & \cdots & \cdots \\ & & \vdots & & \\ a_1 & \cdots & \cdots & \cdots & a_0 \end{bmatrix} \begin{matrix} \leftarrow D \\ \leftarrow D+1 \\ \vdots \\ \\ \end{matrix} \begin{bmatrix} + & + & + & - & + & - & - & - \\ - & + & + & + & - & + & - & - \\ - & - & + & + & + & - & + & - \\ & & & \vdots & & & & \end{bmatrix}$$

Now, any two rows $D+a$ ($(a+1)th\ row$) and $D+b$ ($(b+1)th\ row$) are considered.
Claim : $|(D+a)\cap(D+b)| = \lambda = t^2+t$.

By definition of (v,k,λ)-difference set $b-a$ occurs exactly λ times. Let $g \in (D+a)\cap(D+b)$. Hence, $g = d_1 + a = d_2 + b$ if and only if $d_1 - d_2 = b - a$. This implies that by choosing $d_1 - d_2 = b - a$, then we have an element $g \in (D+a)\cap(D+b)$, thus $|(D+a)\cap(D+b)| = \lambda = t^2+t$.

Let $x_{a,b}$ be the # of pairs $(+1,+1)$ between the two rows.

$y_{a,b}$ be the # of pairs $(+1,-1)$ between the two rows.

$z_{a,b}$ be the # of pairs $(-1,+1)$ between the two rows.

$w_{a,b}$ be the # of pairs $(-1,-1)$ between the two rows.

Since $|(D+a)\cap(D+b)| = 4t^2+t$, $x_{a,b} = t^2+t$.

(1) $x_{a,b} + y_{a,b} + z_{a,b} + w_{a,b} = 4t^2$

$x_{a,b} + z_{a,b} = k = 2t^2+t \quad (+1 \text{ in row } b+1)$

$x_{a,b} + y_{a,b} = k = 2t^2+t \quad (+1 \text{ in row } a+1)$.

$\Rightarrow y_{a,b} = 2t^2 + t - (t^2+t) = t^2 = z_{a,b}$.

By (1) $x_{a,b} + w_{a,b} = 4t^2 - 2t^2 = 2t^2 = y_{a,b} + z_{a,b}$.

Hence, they are orthogonal. □

Remark In fact, this theorem is reversible, i.e., if we have a circulant $\mathcal{H}$-matrix of order $4t^2$, then we have a $(4t^2, 2t^2+t, t^2+t)$-difference set.

Theorem 15.9. Let $D = \{d_1, d_2, \cdots, d_k\}$ be a $(v,k;\Lambda)$-difference set and A_D is the incidence matrix of D. Then, the i^{th} row of $A_D {A_D}^T$ is $(f(\lambda_{1-i}), f(\lambda_{2-i}), \cdots, f(\lambda_{v-i}))$

where $f(x) = v - 4k + 4x$.

Remark $v = 4m,\ k = 2m,\ \lambda_j = \lambda = m$ for $j \in \mathbb{Z}_{4m}$, gives a circulant $\mathcal{H}$-matrix.
($*$) For application on functional magnetic resonance imaging (fMRI), We don't need a circulant $\mathcal{H}$-matrix, a partial circulant $\mathcal{H}$matrix can do the job. In order to obtain better results, we would like to find as many circulant orthogonal vectors as possible.