

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

Notations

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

1. $[n] = \{1, 2, \dots, n\}$.

2. $\binom{[n]}{k} =$ def the collection of k -subsets (all) of $[n]$.

3. $\binom{n}{k} = \left| \binom{[n]}{k} \right|$.

4. $X = \{x_1, x_2, \dots, x_n\}$ is a set of elements and " $\leq$ " is a partial order defined on X . $\langle X, \leq \rangle$ is called a partial ordered set, Poset in short.

(*) " $\leq$ " is a partial order ^{of X} , if (i) $a \leq a \ \forall a \in X$, (ii) $a \leq b$ and $b \leq a$ implies that $a = b$, $\forall a, b \in X$, and (iii) $a \leq b$, $b \leq c$ implies that $a \leq c \ \forall a, b, c \in X$.

(Reflexivity)
(Anti-symmetry)

(Transitivity)

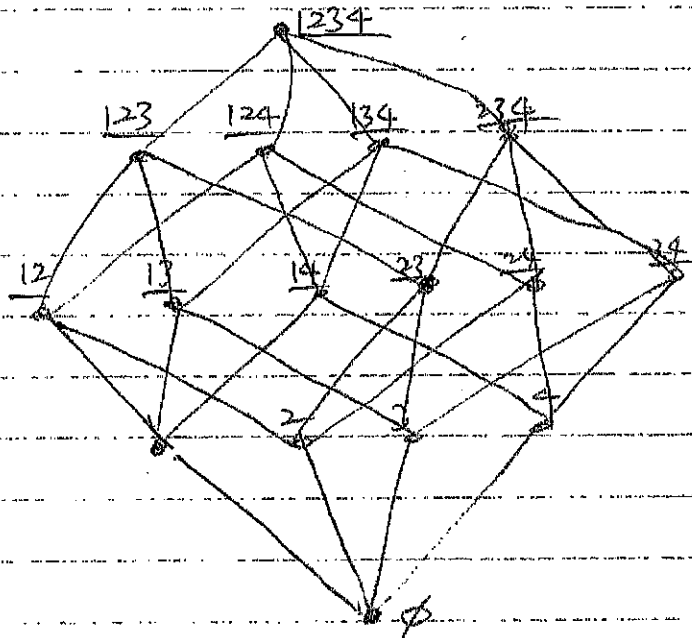
(**) " $\leq$ " is a total order of $\underbrace{Y}_{\text{distinct}}$ provided any two elements

in $\underbrace{Y}_i$, y_i and y_j , either $y_i \leq y_j$ or $y_j \leq y_i$ but not both (y_i and y_j are comparable.)

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

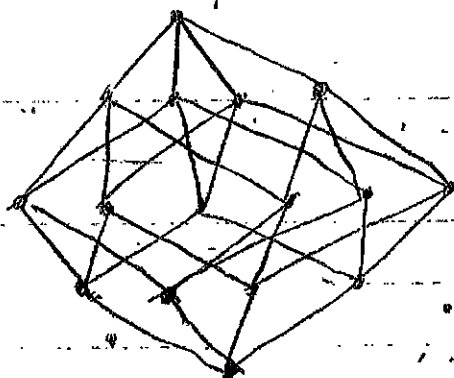


So, for example, $\langle 2^{\{1,2,3,4\}}, \leq \rangle$ can be represented as follows.



For convenience, this diagram can be considered as a

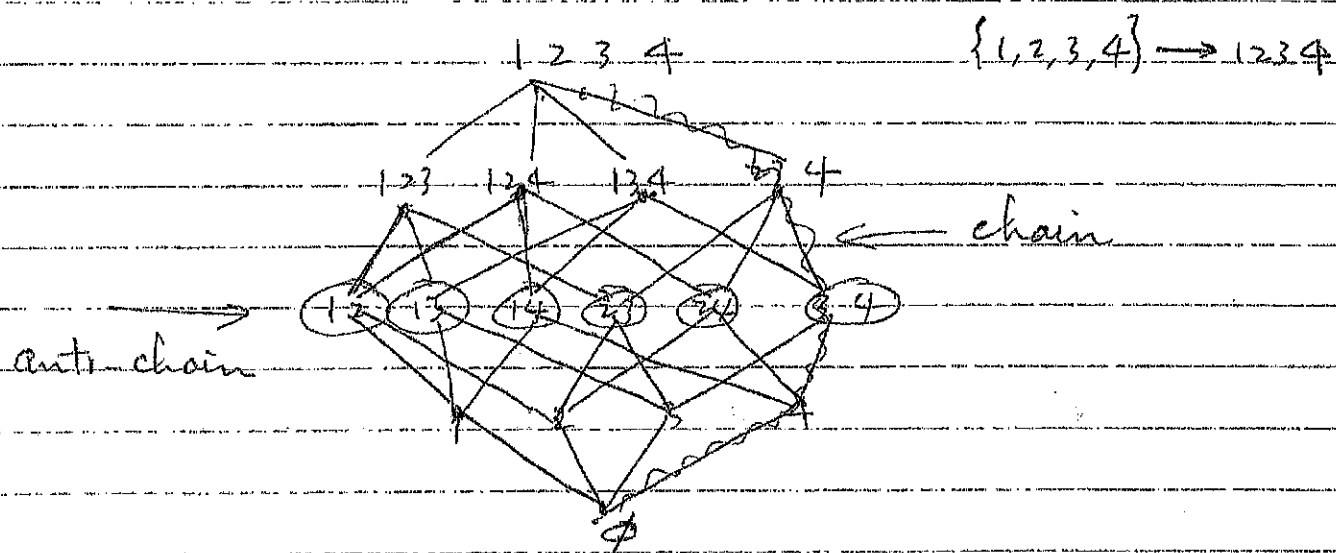
graph:



(*) 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)



Forbidden poset problem

Given a configuration of posets, say $P = I: \begin{array}{c} x \\ | \\ y \end{array} (y \leq x)$,

find the maximum number of sets in $2^{[n]}$ such that the induced partial ordered set contains no sub-poset $(I) \leftarrow$ which is given.

(**) We can change I to $\dots$. For example, $P_3: \begin{array}{c} x \\ | \\ y \end{array}$

or $\begin{array}{c} \vee \\ | \end{array} (Y \text{ or } S_3) \text{ Star}$

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

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 A be the collection of subsets which attains the

maximum. Furthermore, let a_k be the number of sets in A

whose size is k . Hence, $|A| = \sum_{k=0}^n a_k$. (Note that a_k 's may be

zero.) Since $\binom{[n]}{\lfloor \frac{n}{2} \rfloor}$ is clearly an anti-chain, $|A| \geq \binom{n}{\lfloor \frac{n}{2} \rfloor}$. So,

it suffices to prove $|A| \leq \binom{n}{\lfloor \frac{n}{2} \rfloor}$.

Claim (LYM inequality)

Lubell-Yamamoto-Meshalkin

$$\sum_{k=0}^n \frac{a_k}{\binom{n}{k}} \leq 1.$$

Consider the set of permutations of $[n]$. Clearly, there are

$n!$ permutations. Now, for each set S in A , we associate this set with

$|S|!(n-|S|)!$ permutations by taking $\begin{pmatrix} S & [n] \setminus S \\ \alpha(S) & \alpha([n] \setminus S) \end{pmatrix} = \alpha$.

(The first $|S|$ elements of this permutation are exactly S .)

Note that each permutation can only be associated with a single set in A . (?)

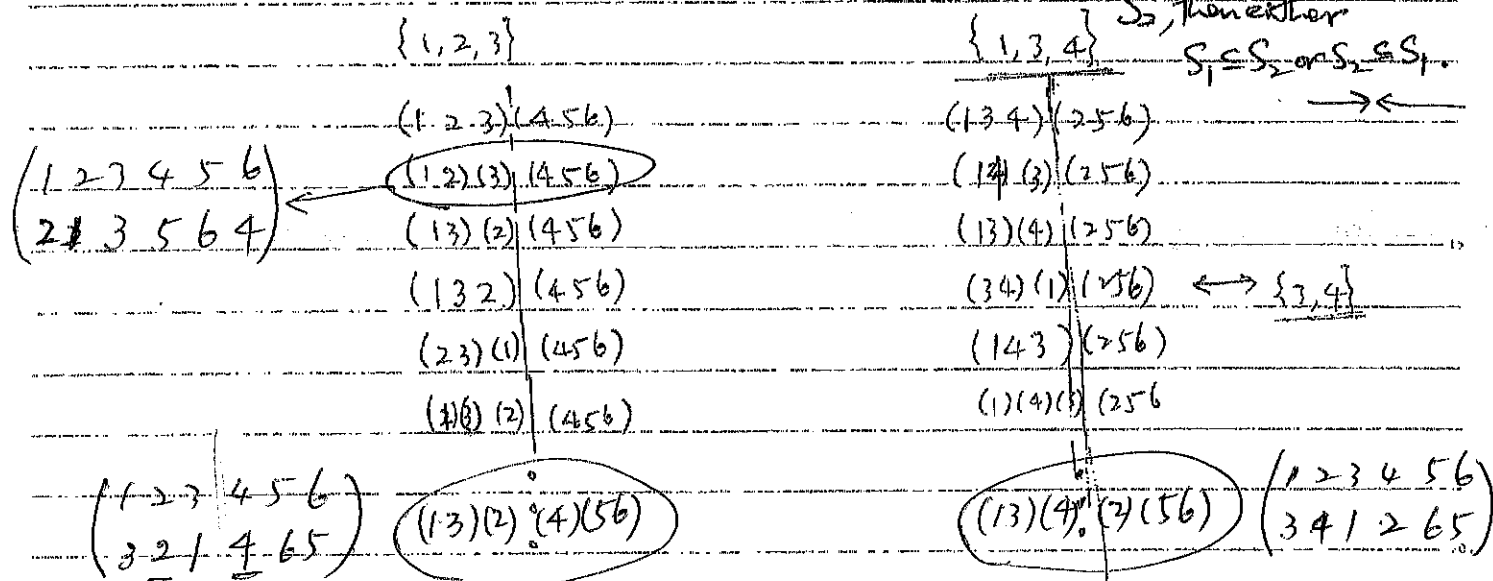
$$\sum_{S \in A} |S|!(n-|S|)! = \sum_{k=0}^n a_k \cdot k!(n-k)! \leq n!$$

This implies that $\sum_{k=0}^n a_k \cdot \frac{k!(n-k)!}{n!} \leq 1$ and the proof follows.

Now, since $1 \geq \sum_{k=0}^n \frac{a_k}{\binom{n}{k}} \geq \sum_{k=0}^n \frac{a_k}{\binom{n}{\lfloor \frac{n}{2} \rfloor}}$, $\binom{n}{\lfloor \frac{n}{2} \rfloor} \geq \sum_{k=0}^n a_k = |A|$.

Example $n=6$

If it associates with two sets S_1 and S_2 , then either $S_1 \subseteq S_2$ or $S_2 \subseteq S_1$.



Exercise 3-6 (5 points)

Find the maximum number of subsets in $2^{[n]}$ such that their

induced poset does not contain P_3 .

A good guess: $\binom{n}{\lfloor \frac{n}{2} \rfloor} + \binom{n}{\lfloor \frac{n}{2} \rfloor + 1}$ (?).

Another beautiful result is the collection of sets, which are

mutually intersecting, i.e., $\forall S_1, S_2 \in \mathcal{B}_{n,r}, S_1 \cap S_2 \neq \emptyset$. $\mathcal{B}_{n,r}$ is
 r -uniform (distinct)
 called an intersecting family defined on $[n]$.

Theorem $|\mathcal{B}_{n,r}| = \binom{n-1}{r-1} \forall n \in \mathbb{N}, r \leq \frac{n}{2}$. (EKR Theorem)

Proof. Let $\mathcal{B} = \{S \mid S \in \binom{[n-1]}{r-1}\}$. Then, $\mathcal{B}$ is an intersecting

family of $[n]$ since each set contains the element n . Hence,

$|\mathcal{B}_{n,r}| \geq \binom{n-1}{r-1}$. Next, we prove that $|\mathcal{B}_{n,r}| \leq \binom{n-1}{r-1}$.

Observe that if we let $(a_1, a_2, \dots, a_n)$ be a cyclic permutation of $[n]$, then this cycle contains at most r sets of $\mathcal{B}_{n,r}$. For

example, $n=8$ and $r=3$, let $(3, 1, 8, 2, 7, 5, 6, 4)$ be an arbitrary

cyclic permutation. Now, if $\{8, 2, 7\} \in \mathcal{B}_{8,3}$, 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 $\mathcal{B}_{n,r}$ can be associate with $r!(n-r)!$

permutations. So, $|\mathcal{B}_{n,r}| \cdot r!(n-r)! \leq r \cdot (n-1)!$, and

thus $|\mathcal{B}_{n,r}| \leq \frac{(n-1)!}{(r-1)!(n-r)!} = \binom{n-1}{r-1}$.

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

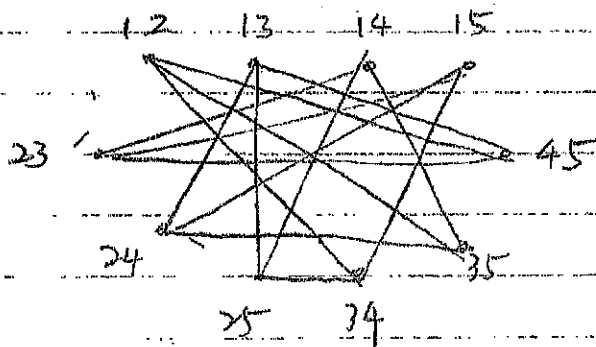
Another good problem to study related to sets.

Let $n = 2t + 1$. Then, 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.

Example $n = 5, t = 2$



This 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.

r-sets in $[n]$

If we further require that any two r -sets can have at most one element in common, thus exactly one element in common, then the collection of such sets (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

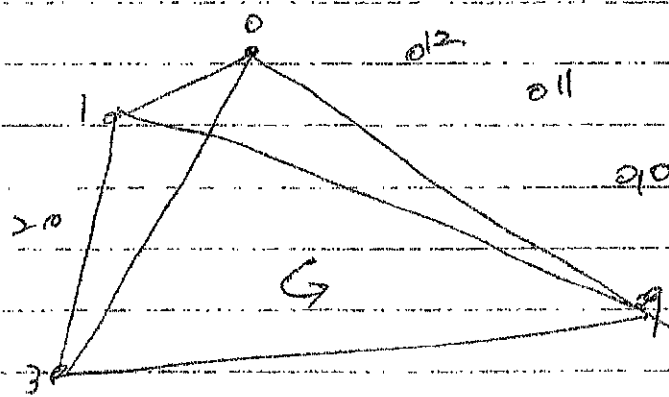
we have in total is $n(n-1)/2 = \binom{n}{2}$ and each r -set can

use $\binom{r}{2} = \frac{r(r-1)}{2}$ pairs, this implies that $|B_{n,r}^{(1)}| \leq \frac{\binom{n}{2}}{\binom{r}{2}}$.

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 $|B_{13,4}^{(1)}| = \frac{13 \cdot 12}{4 \cdot 3} = 13$. $B_{13,4}^{(1)} = \{ \{0, 1, 3, 9\} + i \mid i \in \mathbb{Z}_7 \}$



We can check any two of them have one element in common!

Exercise 4-1 (3 points)

Give five nontrivial examples for $n, r \geq 3$, such that

$$|B_{n,r}^{(1)}| = \binom{n}{2} / \binom{r}{2}.$$

It is also interesting to know: ^{$\bar{B}_{n,r}^{(1)}$} the family that any two r -sets in

$\bar{B}_{n,r}^{(1)}$ intersect at one point, i.e., have a common element. The

examples mentioned in p.8, $B_{7,3}^{(1)}$ and $B_{13,4}^{(1)}$ do have such property.

$B_{13,4}^{(1)} :$

0 1 3 9

1 2 4 10

2 3 5 11

3 4 6 12

4 5 7 0

5 6 8 1

6 7 9 2

7 8 10 3

8 9 11 4

9 10 12 5

10 11 0 6

11 12 1 7

12 0 2 8

Exercise 4-2 (3 points)

Find $\bar{B}_{31,6}^{(1)}$.

Combin. Des.

Exercise 1 Due March 28

1-1 Find a solution for 15 girls problem.

1-2 Show that in a $2-(v, b, r, k, \lambda)$ design,

(1) $bk = vr$, (2) $\lambda(v-1) = r(k-1)$ and (3) $b \geq v$.

1-3 Find a $2-(13, 3, 1)$ design and a $2-(19, 3, 1)$ design.

1-4 Find L_n by using a systematic method. (Bonus point for L_6 . (L_n is the number of distinct Latin squares of order n .)

1-5 For each odd n , construct an idempotent commutative $LS(n)$ and for even n , construct a unipotent commutative $LS(n)$.

(Bonus 1) Use D. Stinson's idea to prove that there do not exist two orthogonal Latin squares of order 6.

1-6 $\forall n \neq 2$, construct an idempotent $LS(n)$, and a unipotent $LS(n)$ for $n \geq 2$.

Exercise 2

Due April 18

- 2-1 prove that "isotopism" is an equivalence relation.
- 2-2 prove that a total symmetric $LS(n)$ is a semi-symmetric $LS(n)$ and also a commutative $LS(n)$. Moreover, prove that an associative quasigroup is a group.
- 2-3 prove that a $LS(m)$ can be embedded in a $LS(n)$ if and only if $n \geq 2m$.
- 2-4 Construct a $LS(12)^L$ such that L is commutative and also with holes of type 2^6 .
- (Bonus) Prove the theorem by Hoffman and Kuhn and then the details of Ryser's theorem.
- 2-5 Prove that if $L_1 \perp L_2$ and $M_1 \perp M_2$, then $L_1 \otimes M_1 \perp L_2 \otimes M_2$.
- 2-6 Prove that if there exist $n-2$ $MOLS(n)$, then we can find $n-1$ $MOLS(n)$.

1

Theorem (Exercise 2-6) (For reference)

If there exist $n-2$ mutually orthogonal Latin squares of order n , then there exist $n-1$ MOLS(n)'s.
(MOLS(n))

Proof. Let $L^{(1)}, L^{(2)}, \dots, L^{(n-2)}$ denote $n-2$ MOLS(n)'s, and for $h=1, 2, \dots, n-2$, $L^{(h)} = [l_{ij}^{(h)}]_{n \times n}$. For convenience, we use the elements in $\{1, 2, \dots, n\}$ for the entries in the following arguments. By the fact that permuting entries of squares will not affect the orthogonality, we assume that the first row of $L^{(1)}, L^{(2)}, \dots, L^{(n-2)}$ be $\langle 1, 2, 3, \dots, n \rangle$. Now, let $L^{(n-1)}$ be defined as follows:

(a) the first row of $L^{(n-1)}$ is $\langle 1, 2, \dots, n \rangle$, and

(b) for $i > 1$, $l_{ij}^{(n-1)} \in \{1, 2, \dots, n\} \setminus (\{j\} \cup \{l_{ij}^{(h)} \mid h=1, 2, \dots, n-2\})$.

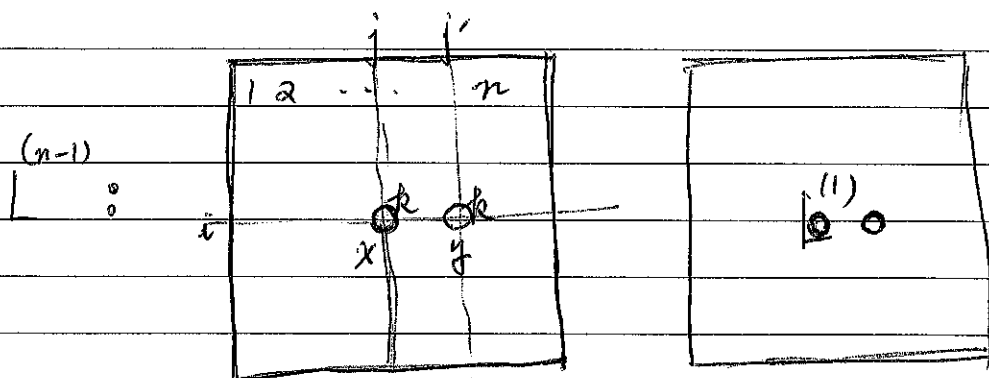
By the fact that $L^{(1)}, L^{(2)}, \dots, L^{(n-2)}$ are mutually orthogonal $l_{ij}^{(h)} \neq l_{ij}^{(h')}$ for $1 \leq h \neq h' \leq n-2$ and $l_{ij}^{(h)} \neq j \forall h \in \{1, 2, \dots, n-2\}$.

Therefore, $l_{ij}^{(n-1)}$ is uniquely determined. It's left to show that $L^{(n-1)}$ is a Latin square and $L^{(n-1)} \perp L^{(h)}$ for $h \in \{1, 2, \dots, n-2\}$.

Claim 1: $L^{(n-1)}$ is a Latin square of order n .

(a) $\forall i = 2, 3, \dots, n-1, l_{ij}^{(n-1)} \neq l_{ij'}^{(n-1)}, 1 \leq j \neq j' \leq n$.

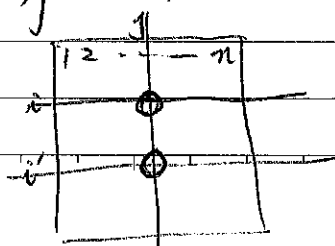
Suppose not. $\exists j \neq j'$, such that $l_{ij}^{(n-1)} = k = l_{ij'}^{(n-1)}$.



In this case, clearly, $i \neq k$. By the definition of $L^{(n-1)}$, the corresponding x, y in $L^{(1)}, L^{(2)}, \dots, L^{(n-2)}$ do not have entry k . ^{Note that} k occurs in the i^{th} row of $L^{(1)}, L^{(2)}, \dots, L^{(n-2)}$ but not in $j^{\text{th}}, j'^{\text{th}}$ and k^{th} column. Moreover, they occur in different columns of $L^{(1)}, L^{(2)}, \dots, L^{(n-2)}$. This is not possible, since _(ith row) we only have $n-3$ choice for $n-2$ k 's. (That is, at least two k 's will occur in the same row and the same column of the $n-2$ $\text{MOLS}(n)$'s, a contradiction.

(b) $\forall j = 1, 2, \dots, n, l_{ij}^{(n-1)} \neq l_{i'j}^{(n-1)}, 2 \leq i \neq i' \leq n$.

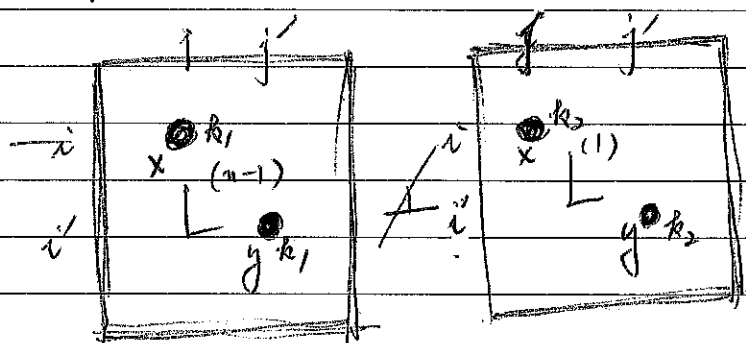
It follows by a similar argument as above.



Claim 2 $L^{(n-1)} \perp L^{(h)} \quad \forall h=1, 2, \dots, n-2$.

Suppose not. For convenience, assume that $L^{(n-1)} \not\perp L^{(1)}$.

(第一个不垂直于 $L^{(n-1)}$ 的方程。) Therefore, there exist i, j, i', j' , $l_{ij}^{(n-1)} = l_{i'j'}^{(n-1)}$ and $l_{ij}^{(1)} = l_{i'j'}^{(1)}$. Obviously, $i \neq i'$, and none of $\{i, i'\}$ is equal to 1. (See it?)



By definition of $L^{(n-1)}$, $l_{ij}^{(n-1)} \neq l_{i'j'}^{(1)}$ (so is $l_{ij}^{(n-1)} \neq l_{i'j'}^{(h)}, h=2, \dots, n-2$).

So, let $l_{ij}^{(n-1)} = k_1 = l_{i'j'}^{(n-1)}$ and $l_{ij}^{(1)} = k_2 = l_{i'j'}^{(1)}$. $k_1 \neq k_2$.

Now, consider the above $L^{(1)}$ and $L^{(2)}, \dots, L^{(n-2)}$. Since they are

mutually orthogonal, in each $L^{(h)}$ (h ≥ 2) the entries in x and y

are different and also they are different from k_2 . Moreover,

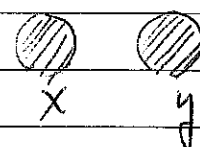
the entry in the j th column is different from j . See next

page for an explanation.

$L^{(1)}$					$L^{(2)}$					$L^{(3)}$				
1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
3	4	5	1	2	4	5	1	2	3	5	1	2	3	4
5	1	2	3	4	2	3	4	5	1	4	5	1	2	3
2	3	4	5	1	5	1	2	3	4	3	4	5	1	2
4	5	1	2	3	3	4	5	1	2	2	3	4	5	1

$L^{(4)}$:

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



Constructed by the above definition.

From $L^{(1)}$, look at all entries "3" in 2-5th row. 对应於 $L^{(2)}$ 与 $L^{(1)}$ 的位置填入 1, 2, 4, 5. 由定义知道填入 $L^{(4)}$ 的 4 个位置都会是不同的元素, 因为 $L^{(4)}$ 是扣掉早已出现的元素, 除了 1 之外各出现 3 次, 其它 3 个位置也依同样规则. 所以当 $L^{(1)}$ 中出现相同的 entries "3", 在 $L^{(1)}$ 中的对应位置将会填入不同的元素; 前面的假设不会成立. 按照上述的推论, $L^{(n-1)} \perp L^{(1)}$.
Similarly, $L^{(n-1)} \perp L^{(h)}$, $h = 2, 3, \dots, n-2$. ▣

Exercise 3

Due May, 9

3-1 Find $\text{Spec}_c(4)$.

3-2 Explain your idea in using Latin squares as keys.

3-3 How to use critical sets for sharing schemes?

3-4 Prove that if L is a Latin square of odd order n ,

then $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes L$ contains no transversals.

3-5 Give examples L' such that $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \otimes L'$ contains a transversal when L' is a Latin square of even order n , $n = 2m$, $m \in \mathbb{N}$.

Bonus prove $|T_n| \geq n - \sqrt{n}$ in details.

Bonus Give an explanation of the work by Pooya Hatami and P. Shor on partial transversal, $|T_n| \geq n - O(\log^2 n)$.

3-6 Find the maximum number of subsets in $2^{[n]}$ such that their induced (graph or poset) does not contain P_3 .