Introduction to Combinatorics Lecture 10

Critical Sets

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

Facts.

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, and was proved by B. Smetaniuk in 1981. You may refer to 'A course in combinatorics' by J.H van Lint and R.M. Wilson, page 189-193.
2. It takes about 50 pages to characterize a $PLS(n)$ with at most $n+1$ filled cells which is in completable. (L.D. Anderson and A.J.W. Hilton, 1983, LMS.)

0	1	2	
			3

0			
	0		
		0	
			1

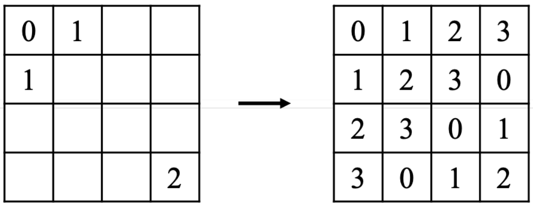
Figure 10.1: n filled cells may be too much!

Definition 10.1 (Critical set)**.** A partial Latin square C is called a critical set of a Latin square L if

1. the empty cells of C can be filled to obtain L, and
2. any proper sub-partial square of C can be completed to at least two distinct Latin squares (one of them is L).

Remark.

- A critical set of order n contains at least $n-1$ distinct elements and covers at least $n-1$ rows and $n-1$ columns.
- Sudoku is a special critical set of order 9.



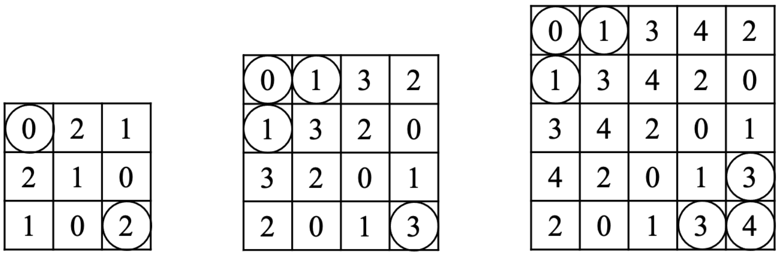
0	1		
1			
			2

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

Figure 10.2: A critical set.

Facts.

3. 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

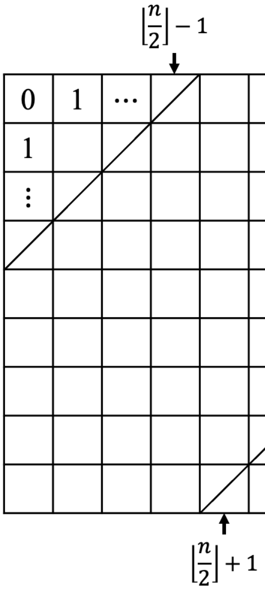

$\lfloor \frac{n}{2} \rfloor - 1$
0
1
⋯
1
⋮
⋮
n-2
⋯
n-2
n-1
$\lfloor \frac{n}{2} \rfloor + 1$

Figure 10.3

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

Conjecture 10.1. $|C| \geq \lfloor \frac{n^2}{4} \rfloor$.

Construction of Latin squares with many subsquares.

First, we consider the operation of two Latin squares.

Definition 10.2 (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 nm 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 $(x, B_{i',j'})$.

Example.

$A:$

0	1
1	0

$B:$

0	1	2
2	0	1
1	2	0

$B':$

0	2	1
2	1	0
1	0	2

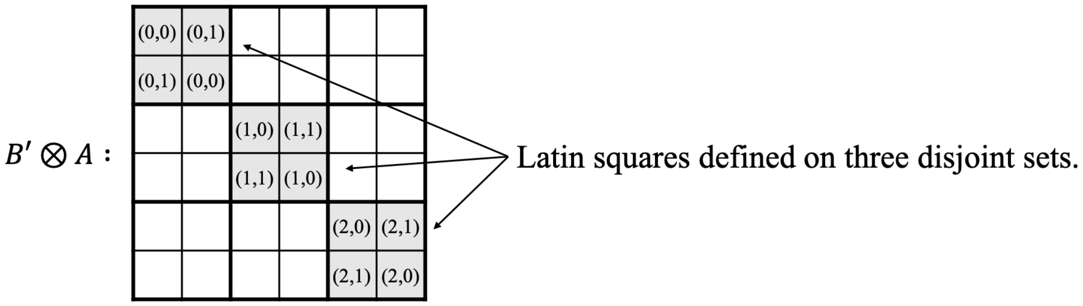
$A \otimes B:$

(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)

$B' \otimes A:$



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

Latin squares defined on three disjoint sets.

Figure 10.4

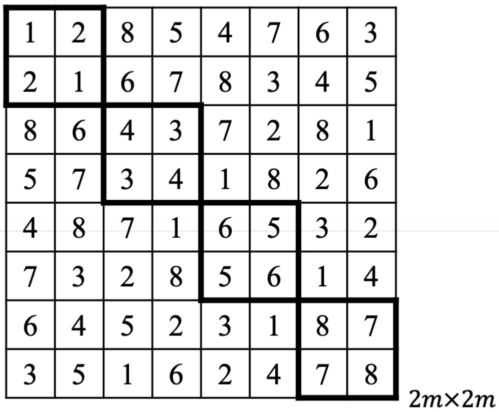
Remark.

- $B' \otimes A$ is referred to as a Latin square with 2×2 holes.
- Let $n = h_1 + h_2 + \cdots + h_t$. If L is a Latin square of order n with t subsquares of order $h_1, h_2, ..., h_t$ (as above), 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 2^6.

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

Example. $m = 4$.



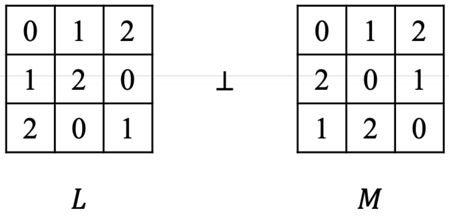
1	2	8	5	4	7	6	3
2	1	6	7	8	3	4	5
8	6	4	3	7	2	8	1
5	7	3	4	1	8	2	6
4	8	7	1	6	5	3	2
7	3	2	8	5	6	1	4
6	4	5	2	3	1	8	7
3	5	1	6	2	4	7	8

Figure 10.5

Orthogonal Latin Squares

Definition 10.3 (Orthogonal Latin squares)**.** 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 $\{(l_{i,j}, m_{i,j}) \mid 1 \le i, j \le n\} = \mathbb{Z}_n^2$, denoted as $L \perp M$.

Example.

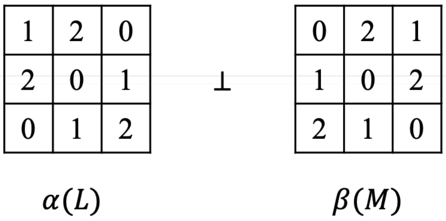


$$\underset{L}{\begin{array}{|c|c|c|}\hline 0&1&2\\\hline 1&2&0\\\hline 2&0&1\\\hline\end{array}} \perp \underset{M}{\begin{array}{|c|c|c|}\hline 0&1&2\\\hline 2&0&1\\\hline 1&2&0\\\hline\end{array}}$$

Figure 10.6

Proposition 10.1. *Let $\alpha(L)$ denote the Latin square which is obtained from L by permuting the entries of L with α (permutation of $\mathbb{Z}_n$). If $L \perp M$, then $\alpha(L) \perp \beta(M)$ for any two permutation α and β for $\mathbb{Z}_n$.*

Example. 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 $\alpha(L) \perp \beta(M)$.



$$\underset{\alpha(L)}{\begin{array}{|c|c|c|}\hline 1&2&0\\\hline 2&0&1\\\hline 0&1&2\\\hline\end{array}} \perp \underset{\beta(M)}{\begin{array}{|c|c|c|}\hline 0&2&1\\\hline 1&0&2\\\hline 2&1&0\\\hline\end{array}}$$

Figure 10.7

Proposition 10.2 (Two Finger's rule)**.** *$L \perp M$ if and only if $y \ne z$ in M whenever their corresponding entries in L are the same entry, i.e., $l_{i,j} = l_{i',j'} \implies m_{i,j} \ne m_{i',j'}$.*

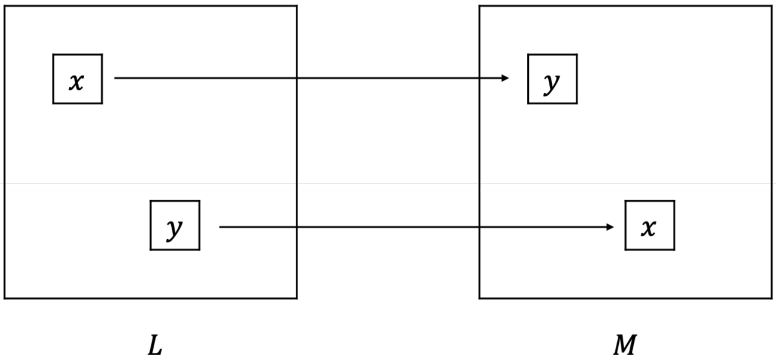


Figure 10.8: Corresponding entries.

Proposition 10.3. *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 $N_1 \perp N_2 \implies (L_1 \otimes M_1) \otimes N_1 \perp (L_2 \otimes M_2) \otimes N_2$ and more.)*

Proposition 10.4. *If n is a prime power, then there exist $n-1$ Latin squares of order n, $L_1, L_2, ..., L_{n-1}$, which are mutually orthogonal, i.e., $L_i \perp L_j$ for any two $1 \leq i \neq j \leq n-1$.*

Proof. Since n is a prime power, we have a finite field $GF(n)$, $\langle F, +, \cdot \rangle$. Let $F^* = F \setminus \{0\}$. For convenience, let $F = \{0 = \alpha_0, \alpha_1, ..., \alpha_{n-1}\}$. Now, for $0 \leq i, j \leq n-1$, we define $L_{i,j}^{(h)} = \alpha_i + \alpha_h \cdot \alpha_j$ where $h \in F^*$. Since $i \neq i'$ implies that $L_{i,j}^{(h)} \neq L_{i',j}^{(h)}$ and $j \neq j'$ implies that $L_{i,j}^{(h)} \neq L_{i,j'}^{(h)}$ 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 $(i, j) \neq (i'j')$, $L_{i,j}^{(h)} = L_{i',j'}^{(h)}$. Consider $1 \leq k \neq h \leq n-1$. Suppose that $L_{i,j}^{(k)} \neq L_{i',j'}^{(k)}$. Then we have

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

$(\alpha_h - \alpha_k)\alpha_j = (\alpha_h - \alpha_k)\alpha_{j'} \implies \alpha_j = \alpha_{j'} \implies \alpha_i = \alpha_{i'}$. A contradiction. Hence, $L^{(h)} \perp L^{(k)}$. □

Facts on finite fields.

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

b. $\langle \mathbb{Z}_n, +, \cdot \rangle$ is a finite field if and only if n is a prime.

c. 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 $g(x)$ (over $\mathbb{Z}_p$) of degree m, i.e., $GF(n) \cong \mathbb{Z}_p[x]/\langle g(x) \rangle$.

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

e. If $\langle F, +, \cdot \rangle$ is a finite field, then $\langle F^*, \circ \rangle$ is a cyclic group, i.e., $\langle F^*, \circ \rangle \cong \langle \alpha \rangle$, F^* is generated by an element $\alpha \in F^*$ $(= F \setminus \{0\})$.

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

Definition 10.4 (A complete family if MOLS(n))**.** For order n, $n-1$ mutually orthogonal Latin squares (MOLS) form a complete family of MOLS(N).

Facts.

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

   Remark.

   - So far, only for prime power n that we can find a complete family of MOLS(n).
   - It is known that there does not exist a complete family of MOLS(n) for $n = 6$ and 10.

   Example. Figure 10.9 is a complete family of MOLS(4). (Can we find the 3rd one by using the first two MOLS(4)?) Note that two mutually orthogonal Latin squares of order 4 solve the 16 cards problem!

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

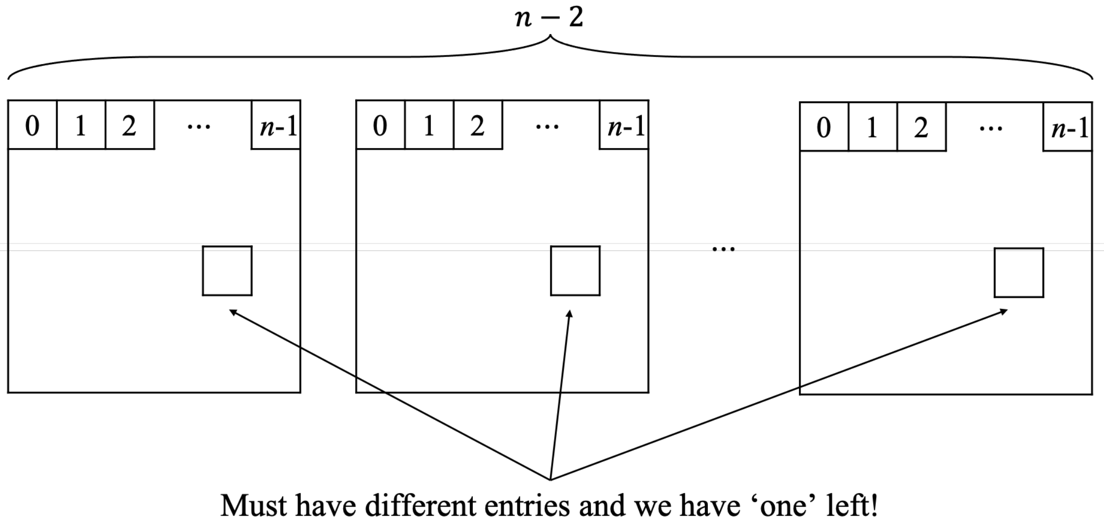
   Proof. By Proposition 10.2, we can assume all mutually orthogonal Latin squares do have the same first row $(0, 1, 2, ..., n-1)$. Then, consider the $(2, 1)$ cell, no two of the squares have the same entry. (?) Hence, we have at most $n-1$ distinct Latin squares which are mutually orthogonal. □

$$\begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline 1 & 0 & 3 & 2 \\ \hline \end{array} \quad \perp \quad \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline 3 & 2 & 1 & 0 \\ \hline \end{array} \quad \underset{?}{\perp} \quad \begin{array}{|c|c|c|c|}\hline 0 & 1 & 2 & 3 \\ \hline 3 & 2 & 1 & 0 \\ \hline 1 & 0 & 3 & 2 \\ \hline 2 & 3 & 0 & 1 \\ \hline \end{array}$$

Figure 10.9: A complete family of MOLS(4).

Proposition 10.5. *If there exist $n-2$ MOLS(n), then we can find $n-1$ MOLS(n).*

Idea of proof.



Must have different entries and we have ‘one’ left!

Figure 10.10

Why Euler made the following conjecture?

Conjecture 10.2 (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 $n \neq 2 \pmod 4$, then either n is a prime or n has a prime factor larger than 2.)*

Facts.

6. Euler’s conjecture is true for $n = 2$ and 6 (only!). Also, $n = 1$ is trivial.

7. 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 10.3, we can construct two MOLS(n) by using direct product of two mutually orthogonal Latin squares of order $2^t, p_1^{e_1}, p_2^{e_2}, ..., p_k^{e_k}$ 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.)

Euler's conjecture was disproved by Parker, Bose and Shrikhande in the year 1959. Figure 10.11 are two MOLS(10) proposed by E. T. Parker. As for $n \equiv 2 \mod 4$, $n \geq 10$, we need to apply ideas from pairwise balanced design to prove that two MOLS(n) do exist. (See lecture notes on Combinatorial Designs, Hung-Lin Fu.)

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

Figure 10.11: Two MOLS(10).

Definition 10.5 (r-orthogonal)**.** Two Latin squares of order n defined on the same set S are r-orthogonal if when they are superimposed, exactly r different order pairs of S^2 occur among the n^2 ordered pairs of entries.

Example. The two Latin squares is a pair of 34-orthogonal Latin squares of order 6. $(3, 4)$ and $(1, 5)$ are the only two repeated ordered pairs.

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

Figure 10.12: A pair of 34-orthogonal Latin squares.

Definition 10.6 (Orthogonal array)**.** An orthogonal array of order n with depth k, $\mathrm{OA}(k, n)$, is a $k \times n^2$ array $A = [a_{i,j}]$ such that for any two rows, the ordered pairs obtained from the two rows are exactly all ordered pairs of $\mathbb{Z}_n^2$ $(a_{i,j} \in \mathbb{Z}_n)$.

Example. OA(4,3).

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

↑

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

Figure 10.13: OA(4,3).

Facts.

8. The existence of an OA(k, n) is equivalence to the existence of $k-2$ MOLS(n). (This fact comes from that the number of ordered pairs is at most n^2.)
9. An OA(k, n) has at most n^2 columns and $n+1$ rows. (This fact is a consequence of the result that there are at most $n-1$ MOLS(n).)

In applications, 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 $n+1$.

Example. $n = 3,\ m = 3,\ k = 5.$

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

Three columns represent three orthogonal partial Latin squares.

Remark. If $m = n^2$, then $k \leq n+1$.