Week 15-16: Combinatorial Design

May 8, 2017

A **combinatorial design**, or simply a **design**, is an arrangement of the objects of a set into subsets satisfying certain prescribed properties. The area of combinatorial design is highly developed, yet many interesting problems and fundamental questions still remain open. Many of the methods for constructing designs rely on the algebraic structure called finite field and more general system of arithmetics.

1 Modular Arithmetic

Let $\mathbb{Z}$ denote the set of all integers, i.e.,

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

We denote by + and × the ordinary addition and multiplication of integers respectively.

Let n be a positive integer with $n \geq 2$ and let

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$$

be the set of nonnegative integers which are less than n. We can think of the integers of the set $\mathbb{Z}_n$ as the possible remainders when any integer is divided by n.

If m is an integer, then there is a unique integers q (the **quotient**) and r (the **remainder**) such that

$$m = q \times n + r, \quad 0 \leq r \leq n-1.$$

Keep this in mind we introduce an **addition**, denoted $\oplus$, and a **multiplication**, denoted $\otimes$, on $\mathbb{Z}_n$ as follows: For any two integers $a, b \in \mathbb{Z}_n$,

$$\begin{aligned} a \oplus b &= \text{the remainder of } a + b \text{ when divided by } n, \\ a \otimes b &= \text{the remainder of } a \times b \text{ when divided by } n. \end{aligned}$$

Example 1.1. For $n = 2$, we have $\mathbb{Z}_2 = \{0, 1\}$, and

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

For $n = 3$, we have $\mathbb{Z}_3 = \{0, 1, 2\}$, and

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

For $n = 6$,

$$\begin{gathered} 4 \oplus 5 = 3, \quad 3 \oplus 4 = 1, \quad 4 \oplus 2 = 0, \\ 4 \otimes 5 = 2, \quad 3 \otimes 4 = 0, \quad 4 \otimes 2 = 2. \end{gathered}$$

2 Block Design

Example 2.1. Suppose there are 7 varieties of a product to be tested for acceptability among consumers. The manufacturer plans to ask some random (or typical) customers to compare the different varieties. Due to time consuming, a customer is not asked to compare all pairs of the varieties. Instead, each customer is asked to compare a certain 3 of the varieties. In order to draw a meaningful conclusion based on statistical analysis of the results, the test is to have the property that each pair of the 7 varieties is compared by exactly one person. Can such a testing experiment be designed?

There are $\binom{7}{2} = 21$ comparisons. Each person can do $\binom{3}{2} = 3$ comparisons. Then $\frac{21}{3} = 7$ person are needed for the design. This means that such a design is possible. Can we actually construct one of such designs? Let us denote the 7 varieties by the set $\{0, 1, 2, \ldots, 6\}$. Then the following is one of such designs.

$$\{0,1,2\},\ \{0,3,4\},\ \{0,5,6\},\ \{1,3,5\},\ \{1,4,6\},\ \{2,3,6\},\ \{2,4,5\}.$$

These subsets are called the *blocks* of the design. Let us denote these block by $B_1, B_2, \ldots, B_7$ respectively. Then there is an **incidence relation** R between the set $\{0, 1, 2, \ldots, 7\}$ and the set $\mathcal{B} = \{B_1, B_2, \ldots, B_7\}$, defined by

$$(a_i, B_j) \in R \quad \text{if} \quad a_i \in B_j.$$

The incidence relation R can be exhibited by the table (or 0-1 matrix)

	B_1	B_2	B_3	B_4	B_5	B_6	B_7
0	1	1	1	0	0	0	0
1	1	0	0	1	1	0	0
2	1	0	0	0	0	1	1
3	0	1	0	1	0	1	0
4	0	1	0	0	1	0	1
5	0	0	1	1	0	0	1
6	0	0	1	0	1	1	0

Let $X = \{x_1, x_2, \ldots, x_v\}$ be a finite set, whose elements are called **varieties**. A **design** on X is a collection $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ of subsets of X; the objects B_i are called **blocks**, and the design is denoted by $(X, \mathcal{B})$. A design $(X, \mathcal{B})$ is called **complete** if $X \in \mathcal{B}$; otherwise, it is called **incomplete**.

A design $(X, \mathcal{B})$ is called **balanced** if any two members $x_i, x_j \in X$ $(i \neq j)$ meet in $\mathcal{B}$ the same number of times, i.e.,

$$\#\big\{B \in \mathcal{B} : \{x_i, x_j\} \subseteq B\big\} = \lambda;$$

the number λ is called the **index of the design**.

A design $(X, \mathcal{B})$ is called a **block design** if all blocks of $\mathcal{B}$ have the same number of elements, i.e., there is a number k such that

$$|B| = k \quad \text{for all} \quad B \in \mathcal{B}.$$

The block design with the parameters v, b, k is also called a (b, v, k)**-design**.

Definition 2.1. Let b, v, k, and λ be positive integers such that

$$v > k \geq 2.$$

Let $(X, \mathcal{B})$ be a block design with

$$X = \{x_1, x_2, \ldots, x_v\}, \quad \mathcal{B} = \{B_1, B_2, \ldots, B_b\}, \quad |B_i| = k \ \ (1 \leq i \leq b).$$

If $(X, \mathcal{B})$ is balanced, then the design is called **balanced incomplete block design** (or **BIBD** for short). For convenience we call such a BIBD a (b, v, k, λ)**-design** or a **BIBD**(b, v, k, λ).

A design $(X, \mathcal{B})$ can be completely described by the **incidence matrix** M, whose rows are indexed by the elements of X and whose columns are indexed by the blocks of $\mathcal{B}$. The entry of the matrix M at (x, B) is defined to be 1 if $x \in B$; otherwise it is defined to be 0.

Theorem 2.2. *Let* $(X, \mathcal{B})$ *be a* BIBD(b, v, k, λ)*. Then each member of* X *meets exactly* r *blocks in* $\mathcal{B}$*. More precisely, for each* $x \in X$*,*

$$|\{B \in \mathcal{B} : x \in B\}| = r \quad \textit{and} \quad r = \frac{\lambda(v-1)}{k-1}.$$

Proof. Let x be a member of X, and let $B_{l_1}, B_{l_2}, \ldots, B_{l_r}$ be the blocks that contain the member x. We define a 0-1 matrix A whose rows are indexed by the members of $X - \{x\}$ and whose columns are indexed by the blocks $B_{l_1}, B_{l_2}, \ldots, B_{l_r}$; an entry (x_i, B_{l_j}) of A is 1 if and only if $x_i \in B_{l_j}$. We count the number of 1's in A in two ways (along the rows and along the columns):

(1) Each member $x_i \in X - \{x\}$ is contained in λ blocks since the pair $\{x, x_i\}$ is contained in λ blocks.

(2) Each block B_{l_j} contains $k - 1$ elements of $X - \{x\}$.

Thus the number of 1's in the matrix A is

$$(v-1)\lambda = (k-1)r.$$

It follows that $r = \frac{\lambda(v-1)}{k-1}$, which is a constant for all $x \in X$. □

There are five parameters b, v, k, r, and λ, not all independent, associated with any BIBD. Their meanings are as follows:

b: the number of blocks;
v: the number of varieties;
k: the number of varieties contained in each block;
r: the number of blocks containing any one particular variety;
λ: the number of blocks containing any one particular pair of varieties.

Corollary 2.3. *In any* BIBD *we have*

$$bk = vr, \quad \lambda < r.$$

Proof. Equality follows from counting the number of 1's in the incidence matrix of the design. As for the inequality, since $k < v$ then $k - 1 < v - 1$, thus

$$r = \frac{\lambda(v-1)}{k-1} > \lambda.$$

□

Example 2.2. Is there any BIBD with the parameters $b = 12$, $v = 16$, $k = 4$, and $r = 3$? If there is such a BIBD then the index of the design is

$$\lambda = \frac{r(k-1)}{v-1} = \frac{3 \times 3}{15} = \frac{3}{5}$$

which is not an integer. Thus there is no BIBD satisfying the given conditions.

Example 2.3. Is there any BIBD with the parameters $b = 12$, $v = 9$, $k = 3$, and $r = 4$, and $\lambda = 1$? If yes, find such a BIBD? Note that

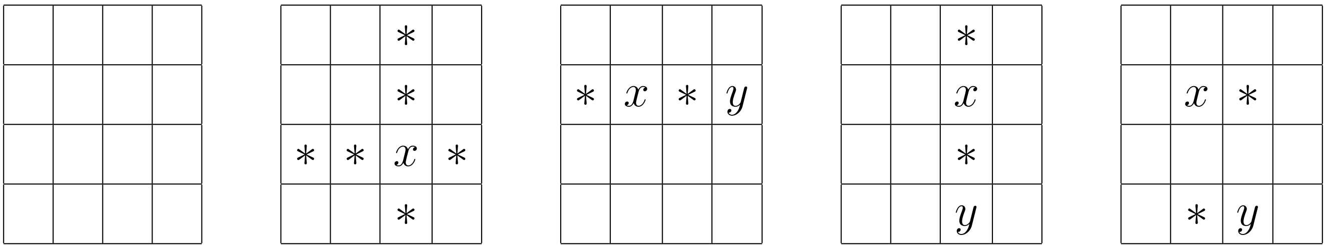
$$r = \frac{\lambda(v-1)}{k-1} = \frac{1 \times (9-1)}{3-1} = 4,$$

$$bk = 12 \times 3 = 9 \times 4 = vr.$$

It seems that there is contradiction. Such a BIBD is displayed by the following incidence matrix:

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

Example 2.4. Let X be the set of the 16 squares of a 4-by-4 board; see below.



For each square $x = (i, j)$, we take the 6 squares which are either in its row or in its column (but not the square itself) to be a block $B_{i,j}$, i.e.,

$$B_x = B(i, j) = \{(i, q) \in X : q \neq j\} \cup \{(p, j) \in X : p \neq i\}.$$

Let $\mathcal{B} = \{B(i, j) : 1 \leq i, j \leq 4\}$. Then $(X, \mathcal{B})$ is a BIBD with parameters $b = 16$, $v = 16$, $k = 6$, $r = 6$, and $\lambda = 2$. In fact, for any two squares $x, y \in X$, there are two blocks shown above that contain both x and y. Thus $(X, \mathcal{B})$ is a BIBD. Moreover, $b = v$.

Theorem 2.4 (Fisher's Inequality). *For any* BIBD *we have*

$$b \geq v.$$

Proof. Let A be the v-by-b incidence matrix of a BIBD. Since each variety belongs to r blocks and each pair of varieties is contained in λ blocks, then the (x, y)-entry of AA^T is

$$\sum_{B \in \mathcal{B}} a_{xB} a_{yB} = |\{B \in \mathcal{B} : x, y \in B\}| = \begin{cases} r & \text{if } \ x = y \\ \lambda & \text{if } \ x \neq y \end{cases}$$

where $a_{xB} = 1$ if $x \in B$ and $a_{xB} = 0$ if $x \notin B$. In other words, the v-by-v matrix AA^T has the form

$$AA^T = \begin{bmatrix} r & \lambda & \cdots & \lambda \\ \lambda & r & \cdots & \lambda \\ \vdots & \vdots & \ddots & \lambda \\ \lambda & \lambda & \cdots & r \end{bmatrix}$$

It is clear that $\det(AA^T) \neq 0$. Then the column vectors of AA^T are linearly independent. It follows that the column vectors of A^T are linearly independent, i.e., the row vectors of A are linearly independent. So the rank of A is v. Thus $v \leq b$. □

Definition 2.5. A BIBD is called **symmetric** if $b = v$, i.e., its incidence matric is a square matrix. A symmetric BIBD is often called an **SBIBD** for short.

An SBIBD can be constructed as follows: Start with a set $\mathbb{Z}_v = \{0, 1, 2, \ldots, v-1\}$; take a k-subset B of $\mathbb{Z}_v$. Then for each $i \in \mathbb{Z}_v$, the translate $i + B$ is also a k-subset of $\mathbb{Z}_v$. The subsets

$$B, \quad B+1, \quad B+2, \quad \ldots, \quad B+v-1$$

are called the **blocks developed from** B and the set B is called the **starter block**. If the collection $\mathcal{B} = \{B, B+1, B+2, \ldots, B+v-1\}$ is a BIBD, then it is an SBIBD with parameters $b = v$, $k = r$, and $\lambda = \frac{k(k-1)}{v-1}$.

Example 2.5. Let $v = 7$. Consider $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and the starter block $B = \{0, 1, 3\}$. Then the blocks

$$\begin{aligned} &B+0 = \{0,1,3\},\ B+1 = \{1,2,4\},\ B+2 = \{2,3,5\}, \\ &B+3 = \{3,4,6\},\ B+4 = \{4,5,0\},\ B+5 = \{5,6,1\}, \\ &B+6 = \{6,0,2\} \end{aligned}$$

developed from the starter block B is an SBIBD with $b = v = 7$, $k = r = 3$, and $\lambda = 1$. However, the blocks

$$\begin{aligned} &B+0 = \{0,1,4\},\ B+1 = \{1,2,5\},\ B+2 = \{2,3,6\}, \\ &B+3 = \{3,4,0\},\ B+4 = \{4,5,1\},\ B+5 = \{5,6,2\}, \\ &B+6 = \{6,0,3\} \end{aligned}$$

developed from the starter block $B = \{0, 1, 4\}$ is *not* a BIBD. (The pair $\{0, 1\}$ is contained in one block while the pair $\{0, 3\}$ is contained in two blocks.)

Definition 2.6. Let B be a k-subset of $\mathbb{Z}_v$. The set B is called a **difference set** if each nonzero element of $\mathbb{Z}_v$ appears the same number λ of times among the $k(k-1)$ differences among distinct elements of B, i.e., each element $a \in \mathbb{Z}_v$ $(a \neq 0)$ appears λ times in the *multiset*

$$\Delta(B) = \{x - y : \ (x, y) \in B \times B, \, x \neq y\}.$$

Example 2.6. The subset $B = \{0, 1, 3\}$ of $\mathbb{Z}_7 = \{0, 1, 2, \ldots, 6\}$ is a difference set. In fact, each nonzero element of $\mathbb{Z}_7$ appears exactly once in the following table

$-$	0	1	3
0	0	6	4
1	1	0	5
3	3	2	0

However, the subset $B = \{0, 1, 4\}$ is not a difference set because, for instance, the element 3 appears twice but the element 5 appears zero times in the following table

$-$	0	1	4
0	0	6	3
1	1	0	4
4	4	3	0

Theorem 2.7. *Let B be a k-subset of $\mathbb{Z}_v$ and $k < v$. If B is a difference set, then the blocks developed from B as a starter block forms an* SBIBD *with the index*

$$\lambda = \frac{k(k-1)}{v-1}.$$

Proof. It is enough to show that each pair of elements of $\mathbb{Z}_v$ is contained in the same number of blocks. Since B is a difference set, each nonzero element of $\mathbb{Z}_v$ appears the same number λ of times in the set $\Delta(B)$. Since there are $v - 1$ nonzero elements in $\mathbb{Z}_v$ and $|\Delta(B)| = k(k-1)$, then

$$\lambda(v-1) = k(k-1).$$

Now fix two elements p, q of $\mathbb{Z}_v$ and $p \neq q$. The equation

$$x - y = p - q$$

has $\lambda = \frac{k(k-1)}{v-1}$ solutions in B. For each (x, y) of the λ solutions, let $j = p - x$. Then

$$p = x + j \quad \text{and} \quad q = y + p - x = y + j.$$

This means that $\{p, q\} \subseteq B + j$, where $j = p - x = q - y$ has λ choices. So there are exactly λ blocks of $\mathcal{B}$ containing the subset $\{p, q\}$. □

The inverse of the theorem is *not* true, i.e., an SBIBD need not be developed from any of its block.

Example 2.7. The following collection

$$\{0, 1, 2\},\ \{0, 3, 4\},\ \{0, 5, 6\},\ \{1, 3, 5\},\ \{1, 4, 6\},\ \{2, 3, 6\},\ \{2, 4, 5\}$$

of subsets of $\{0, 1, 2, \ldots, 6\}$ is an SBIBD with the parameters

$$b = v = 7, \quad k = r = 3, \quad \lambda = 1.$$

However, $\mathcal{B}$ is not developed from any of its block. None of the blocks is a difference set.

Example 2.8. Find a difference set B of size 5 in $\mathbb{Z}_{11}$. Choose $B = \{0, 2, 3, 4, 8\}$; the differences of B are displayed by the table

$-$	0	2	3	4	8
0	0	9	8	7	3
2	2	0	10	9	5
3	3	1	0	10	6
4	4	2	1	0	7
8	8	6	5	4	0

where the nonzero elements $1, 2, \ldots, 10$ appear exactly twice. So B is a difference set and generates an SBIBD with $b = v = 11$, $k = r = 5$, and $\lambda = 2$:

$$\begin{aligned}
&B + 0 = \{0, 2, 3, 4, 8\}, && B + 1 = \{1, 3, 4, 5, 9\}, && B + 2 = \{2, 4, 5, 6, 10\},\\
&B + 3 = \{3, 5, 6, 7, 0\}, && B + 4 = \{4, 6, 7, 8, 1\}, && B + 5 = \{5, 7, 8, 9, 2\},\\
&B + 6 = \{6, 8, 9, 10, 3\}, && B + 7 = \{7, 9, 10, 0, 4\}, && B + 8 = \{8, 10, 0, 1, 5\},\\
&B + 9 = \{9, 0, 1, 2, 6\}, && B + 10 = \{10, 1, 2, 3, 7\}
\end{aligned}$$

3 Steiner Triple Systems

Let $\mathcal{B}$ be a BIBD with parameters b, v, k, r, and λ. Assume $k = 2$, i.e., each block contains exactly two elements. Then each pair of two elements can occur at most once in the blocks. Since each pair appears the same number λ of times in the blocks, it turns out that the collection of blocks must be the collection $\mathcal{P}_2(S)$ of all 2-subsets of a set S, and $\lambda = 1$. So all BIBDs with $k = 2$ are trivial and unique. The smallest (in terms of block size) interesting BIBDs are those with $k = 3$. Balanced bock designs with the block size $k = 3$ are called **Steiner triple systems** (**STS** for short).

Example 3.1. Let $X = \{0, 1, 2\}$ and $\mathcal{B}$ the collection with the only subset $\{0, 1, 2\}$. Then $(X, \mathcal{B})$ is a Steiner triple system. This STS is a complete block design with $b = 1$, $v = 3$, $k = v = 3$, and $\lambda = 1$. This is the only Steiner triple system that is *not* a BIBD; all other Steiner triple systems are BIBD.

Example 3.2. Let $X = \{0, 1, 2, \ldots, 6\}$ and let $\mathcal{B}$ be the collection

$$\{0, 1, 2\},\ \{0, 3, 4\},\ \{0, 5, 6\},\ \{1, 3, 5\},\ \{1, 4, 6\},\ \{2, 3, 6\},\ \{2, 4, 5\}.$$

Then $(X, \mathcal{B})$ is a Steiner triple system, and is also an SBIBD.

Example 3.3. The following collection

$$\begin{array}{cccccc} \{0,1,2\} & \{3,4,5\} & \{6,7,8\} & \{0,3,6\} & \{1,4,7\} & \{2,5,8\} \\ \{0,4,8\} & \{2,3,7\} & \{1,5,6\} & \{0,5,7\} & \{1,3,8\} & \{2,4,6\} \end{array}$$

is a Steiner triple system on $\mathbb{Z}_9$ with $b = 12$, $v = 9$, $r = 4$, and $\lambda = 1$.

Theorem 3.1. *Let $\mathcal{B}$ be a Steiner triple system with parameters b, v, and λ. Then*

$$r = \frac{\lambda(v-1)}{2} \quad \textit{and} \quad b = \frac{\lambda v(v-1)}{6}.$$

Moreover, if $\lambda = 1$, then there is nonnegative integer n such that

$$\textit{either} \quad v = 6n + 1 \quad \textit{or} \quad v = 6n + 3.$$

Proof. Since $k = 3$ and $r = \frac{\lambda(v-1)}{k-1}$ by Theorem 2.2, it is obvious that $r = \frac{\lambda(v-1)}{2}$. Since $bk = vr$ by Corollary 2.3, we have

$$b = \frac{vr}{k} = \frac{\lambda v(v-1)}{k(k-1)} = \frac{\lambda v(v-1)}{6}.$$

If $\lambda = 1$, then $v - 1 = 2r$ is even, so v is odd. Since $v(v-1) = 6b$ is a multiple of 6, we conclude that either 3 divides v or 3 divides $v - 1$.

Case 1: 3 divides $v - 1$. Since $v - 1$ is even, then $v - 1$ is a multiple of 6, i.e., there is nonnegative integer n such that $v - 1 = 6n$. Thus $v = 6n + 1$.

Case 2: 3 divides v. Since v is odd, then v is 3 times an odd number, i.e., $v = 3(2n + 1)$ for nonnegative integer n. Thus $v = 6n + 3$. □

Is it possible for each $n \geq 0$ to construct a Steiner triple systems with $v = 6n+1$ and $v = 6n+3$ varieties? For $n = 0$, it is obvious that there is no Steiner triple system with $v = 1$ variety. However, except this trivial case, Kirkman showed that for each $n \geq 0$ the Steiner systems can be constructed with $6n + 1$ and $6n + 3$ varieties.

Theorem 3.2. *If there are Steiner triple systems of index $\lambda = 1$ with v and w varieties respectively, then there is a Steiner triple system of index $\lambda = 1$ with vw varieties.*

Proof. Let $\mathcal{B}_1$ be a Steiner triple system of index $\lambda = 1$ on a set $X = \{a_1, a_2, \ldots, a_v\}$ and let $\mathcal{B}_2$ be a Steiner triple system of index $\lambda = 1$ on a set $Y = \{b_1, b_2, \ldots, b_w\}$. Consider the set $Z = \{c_{ij} : 1 \leq i \leq v,\ 1 \leq j \leq w\}$ and the v-by-w matrix

$$C = \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1w} \\ c_{21} & c_{22} & \cdots & c_{2w} \\ \vdots & \vdots & \ddots & \vdots \\ c_{v1} & c_{v2} & \cdots & c_{vw} \end{bmatrix}$$

whose rows are indexed from 1 to v and whose column is indexed from 1 to w. Let $\mathcal{B}$ be the collection of triples $\{c_{il}, c_{jm}, c_{kn}\}$ satisfying of the following three conditions:

(i) $l = m = n$ and $\{a_i, a_j, a_k\} \in \mathcal{B}_1$, i.e., the entries c_{il}, c_{jm}, c_{kn} lie in the same column of C and $\{a_i, a_j, a_k\}$ is a block in $\mathcal{B}_1$.

(ii) $i = j = k$ and $\{b_l, b_m, b_n\} \in \mathcal{B}_2$, i.e., the entries c_{il}, c_{jm}, c_{kn} lie in the same row of C and $\{b_l, b_m, b_n\}$ is a block in $\mathcal{B}_2$.

(iii) $\{a_i, a_j, a_k\} \in \mathcal{B}_1$ and $\{b_l, b_m, b_n\} \in \mathcal{B}_2$, i.e., the entries c_{il}, c_{jm}, c_{kn} lie be in different rows and different columns of C, $\{a_i, a_j, a_k\}$ is block of $\mathcal{B}_1$ and $\{b_l, b_m, b_n\}$ is a block of $\mathcal{B}_2$.

The above three conditions imply that the triples $\{c_{il}, c_{jm}, c_{kn}\}$ can not lie either in exactly two rows or in exactly two columns. We claim that $\mathcal{B}$ is a Steiner triple system of index $\lambda = 1$. Let c_{il}, c_{jm} be distinct elements of Z. We need to show that there is exactly one element c_{kn} of Z such that $\{c_{il}, c_{jm}, c_{kn}\}$ is a triple of $\mathcal{B}$. We divide the situation into three cases:

Case 1: $l = m$ and $i \neq j$. Since $a_i \neq a_j$ and $\mathcal{B}_1$ is a Sterner triple system of index $\lambda = 1$, there is a unique triple $\{a_i, a_j, a_k\} \in \mathcal{B}_1$ that contains the pair a_i, b_j. Hence $\{c_{il}, c_{jl}, c_{kl}\}$ is the unique triple of $\mathcal{B}$ that contains the pair c_{il}, c_{jl}.

Case 2: $i = j$ and $l \neq m$. Since $b_l \neq b_m$ and $\mathcal{B}_2$ is a Steiner system of index $\lambda = 1$, there is a unique triple $\{b_l, b_m, b_n\} \in \mathcal{B}_2$ that contains the pair b_l, b_m. Hence $\{c_{il}, c_{im}, c_{in}\}$ is the unique triple of $\mathcal{B}$ that contains the pair c_{il}, c_{im}.

Case 3: $i \neq j$ and $l \neq m$. Since $a_i \neq a_j$ and $b_l \neq b_m$, there is a unique triple $\{a_i, a_j, a_k\} \in \mathcal{B}_1$ that contains the pair a_i, a_j, and a unique triple $\{b_l, b_m, b_n\} \in \mathcal{B}_2$ that contains the pair b_l, b_m. There is a unique triple $\{c_{il}, c_{jm}, c_{kn}\} \in \mathcal{B}$ that contains the pair c_{il}, c_{jm}.

We thus have proved that $\mathcal{B}$ is a Steiner triple system of index $\lambda = 1$ with vw varieties. □

Example 3.4. Let $\mathcal{B}_1$ and $\mathcal{B}_2$ be the Steiner triple systems of index $\lambda = 1$ with 3 varieties. Then $\mathcal{B}_1$ and $\mathcal{B}_2$ must be trivial, i.e., $\mathcal{B}_1 = \{a_1, a_2, a_3\}$ and $\mathcal{B}_2 = \{b_1, b_2, b_3\}$. Let C be the matrix whose entries are c_{ij} with $1 \leq i, j \leq 3$. By Theorem 3.2, a Steiner triple system $\mathcal{B}$ on Z can be constructed as follows:

(i) The three rows of the matrix C:

$$\{c_{11}, c_{12}, c_{13}\}, \quad \{c_{21}, c_{22}, c_{23}\}, \quad \{c_{31}, c_{32}, c_{33}\}.$$

(ii) The three columns of the matrix C:

$$\{c_{11}, c_{21}, c_{31}\}, \quad \{c_{12}, c_{22}, c_{32}\}, \quad \{c_{13}, c_{23}, c_{33}\}.$$

(iii) The six triples whose elements are in different rows and different columns of C:

$$\{c_{11}, c_{22}, c_{33}\}, \ \{c_{11}, c_{23}, c_{32}\}, \ \{c_{12}, c_{21}, c_{33}\},$$
$$\{c_{12}, c_{23}, c_{31}\}, \ \{c_{13}, c_{21}, c_{32}\}, \ \{c_{13}, c_{22}, c_{31}\}.$$

If we write $c_{11}, c_{21}, c_{31}, c_{12}, c_{22}, c_{32}, c_{13}, c_{23}, c_{33}$ as $0, 1, 2, \ldots, 8$, then the Steiner triple system becomes

$$\begin{array}{cccc}
\{0,1,2\} & \{0,3,6\} & \{0,4,8\} & \{0,5,7\} \\
\{3,4,5\} & \{1,4,7\} & \{2,3,7\} & \{1,3,8\} \\
\{6,7,8\} & \{2,5,8\} & \{1,5,6\} & \{2,4,6\}
\end{array}$$

The above Steiner triple system $\mathcal{B}$ with parameter $b = 12$, $v = 9$, $k = r = 3$, and $\lambda = 1$ is partitioned into 4 parts, each part is a partition of the set $\{0, 1, 2, \ldots, 8\}$ of varieties. A Steiner triple system $\mathcal{B}$ on a set X with $\lambda = 1$ is called *resolvable* if $\mathcal{B}$ can be partitioned into parts so that each part is a partition of the set X; each part is called a *resolubility class*. A resolvable Steiner triple systems with index $\lambda = 1$ is also called a *Kirkman triple system.*

Example 3.5 (Kirkman's Schoolgirl Problem)**.** A schoolmistress takes her class of 15 girls on a daily walk. The girls are arranged in 5 rows, with 3 girls in each row, so that each girl has 2 companions. Is it possible to arrange such a walk for 7 consecutive days so that no girl will walk with any of her classmates in a row more than once (no two girls are arranged in a row more than once)?

If such a walk is possible, then there are $5\times 7 = 35$ different rows. The problem asks whether there exists a resolvable Steiner triple system with parameters $b = 35$, $v = 15$, $k = 3$, $r = 7$, and $\lambda = 1$. Such a Steiner triple system does exists and one of them is displayed as follows:

$$\begin{array}{lllllll}
\{0,1,2\} & \{0,3,4\} & \{0,5,6\} & \{0,7,8\} & \{0,9,10\} & \{0,11,12\} & \{0,13,14\} \\
\{3,7,11\} & \{1,7,9\} & \{1,8,10\} & \{1,11,13\} & \{1,12,14\} & \{1,3,5\} & \{1,4,6\} \\
\{4,9,14\} & \{2,12,13\} & \{2,11,14\} & \{2,4,5\} & \{2,3,6\} & \{2,8,9\} & \{2,7,10\} \\
\{5,10,12\} & \{5,8,14\} & \{3,9,13\} & \{3,10,14\} & \{4,8,11\} & \{4,10,13\} & \{3,8,12\} \\
\{6,8,13\} & \{6,10,11\} & \{4,7,12\} & \{6,9,12\} & \{5,7,13\} & \{6,7,10\} & \{5,9,11\}
\end{array}$$

Proposition 3.3. *For any Kirkman triple system with parameters $b, v, k, r,$ and λ, there exists a nonnegative integer n such that*

$$\begin{aligned}
v &= 6n+3, \\
b &= (2n+1)(3n+1), \\
k &= 3, \\
r &= 3n+1, \\
\lambda &= 1.
\end{aligned}$$

The number of resolubility classes is

$$\frac{v}{3} = 2n + 1.$$

Proof. Since each resolubility class is a partition of the set of varieties, then v is a multiple of 3. Note that $v = 6n + 1$ or $v = 6n + 3$ for some nonnegative inter n. Then we must have $v = 6n + 3$. Thus

$$b = \frac{v(v-1)}{6} = (2n+1)(3n+1) \quad \text{and} \quad r = \frac{v}{2} = 3n + 1.$$

□

The generalized Kirkman's schoolgirl problem is that whether there exists a Kirkman triple system with $v = 6n + 3$ for each nonnegative integer n. The problem was solved by Ray-Chaudhuri and Wilson after it was posted over one hundred years.

4 Latin Squares

Definition 4.1. Let n be a positive integer and let S be a set of n distinct elements. A **Latin square of order** n (based on S) is an n-by-n matrix whose entries are elements of S such that all rows and columns are permutations of S. We usually take the set $S = \{0, 1, 2, \ldots, n-1\}$.

Let $A = [a_{ij}]$ be a Latin square of order n based on the set $S = \{0, 1, 2, \ldots, n-1\}$. For each integer k ($0 \leq k \leq n-1$), we denote by $A(k)$ the set of positions of k in the matrix A, i.e.,

$$A(k) = \{(i, j) \in S \times S : a_{ij} = k\}.$$

The set $A(k)$ can be considered as an arrangement of n non-attacking rooks on an n-by-n board. Thus the Latin square A produces to a partition

$$A(0), \quad A(1), \quad A(2), \quad \ldots, \quad A(n-1)$$

of $S \times S$, each consisting of n positions for non-attacking rooks. For integers $i, j \in S$ ($i \neq j$), when all positions in $A(i)$ are replaced with j and all positions of $A(j)$ are replaced by i, then we obtain a new Latin square, having the same partition into non-attacking rooks. There are exactly $n!$ Latin squares of order n corresponding to one partition of the board $S \times S$ into non-attacking rook arrangements.

A Latin square of order n is called in *standard form* if its first row is $[0, 1, 2, \ldots, n-1]$. Using the idea of interchanging the positions occupied by various elements $0, 1, 2, \ldots, n-1$ we can always transform a Latin square of order n to standard form.

Theorem 4.2. *Let A be an n-by-n matrix whose (i, j) entry a_{ij} is given by*

$$a_{ij} = i + j \pmod{n}.$$

Then A is a Latin square of order n based on $\mathbb{Z}_n$.

Proof. Fix the ith row, if two entries a_{ij} and a_{ik} are the same, then

$$i + j = a_{ij} = a_{ik} = i + k \pmod{n}.$$

Then $j = k \pmod{n}$. Since $0 \le j, k \le n-1$, we have $j = k$. So the ith row is a permutation of $\mathbb{Z}_n$. Similarly, the jth column is also a permutation of $\mathbb{Z}_n$. □

Theorem 4.3. *Let n be a positive integer and let r be a nonzero integer such that* $\gcd(r, n) = 1$. *Let A be an n-by-n matrix whose (i, j) entry a_{ij} is given by*

$$a_{ij} = r \times i + j \pmod{n}.$$

Then A is a Latin square of order n based on $\mathbb{Z}_n$. Such Latin squares are denoted by L_n^r.

Proof. For any two entries a_{ij} and a_{ik} in the ith row, if $a_{ij} = a_{ik} \pmod{n}$, i.e.,

$$r \times i + j = r \times i + k \pmod{n},$$

then $j = k \pmod{n}$. Since $0 \le j, k \le n-1$, we have $j = k$. So the ith row is a permutation of $\mathbb{Z}_n$.

For two entries a_{ij} and a_{kj} in the jth column, if $a_{ij} = a_{kj}$, i.e.,

$$r \times i + j = r \times k + j \pmod{n},$$

then $rtimesi = r \times k \pmod{n}$. Since r is invertible, we have $i = k \pmod{n}$. Thus $i = k$ since $0 \le i, k \le n-1$. This means that the jth column is a permutation of $\mathbb{Z}_n$. □

Example 4.1. Consider $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. The 6-by-6 matrix

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 5 & 0 & 1 & 2 & 3 & 4 \\ 4 & 5 & 0 & 1 & 2 & 3 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 2 & 3 & 4 & 5 & 0 & 1 \\ 1 & 2 & 3 & 4 & 5 & 0 \end{bmatrix},$$

whose (i, j) entry is defined by $a_{ij} = 5 \times i + j \pmod 6$, is a Latin square of order 6. (5 is invertible modulo 6.) However, the 6-by-6 matrix

$$\begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 0 & 1 & 2 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 0 & 1 & 2 \end{bmatrix},$$

whose (i, j) entry $a_{ij} = 3 \times i + j \pmod 6$, is a not a Latin square. (3 is not invertible modulo 6.)

Let A and B m-by-n matrices, where

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{m1} & b_{m2} & \cdots & b_{mn} \end{bmatrix}.$$

The *juxtaposition* of A and B is the m-by-n matrix

$$A \times B = \begin{bmatrix} (a_{11}, b_{11}) & (a_{12}, b_{12}) & \cdots & (a_{1n}, b_{1n}) \\ (a_{21}, b_{21}) & (a_{22}, b_{22}) & \cdots & (a_{2n}, b_{2n}) \\ \vdots & \vdots & & \vdots \\ (a_{m1}, b_{m1}) & (a_{m2}, b_{m2}) & \cdots & (a_{mn}, b_{mn}) \end{bmatrix}.$$

Theorem 4.4. *Let R_n and S_n be n-by-n matrices defined:*

$$R_n = \begin{bmatrix} 0 & 0 & \cdots & 0 \\ 1 & 1 & \cdots & 1 \\ \vdots & \vdots & & \vdots \\ n-1 & n-1 & \cdots & n-1 \end{bmatrix} \quad \textit{and} \quad S_n = \begin{bmatrix} 0 & 1 & \cdots & n-1 \\ 0 & 1 & \cdots & n-1 \\ \vdots & \vdots & & \vdots \\ 0 & 1 & \cdots & n-1 \end{bmatrix}.$$

Let $A = [a_{ij}]$ be an n-by-n matrix A based on $\mathbb{Z}_n$. The A is a Latin square if and only if the juxtapositions $R_n \times A$ and $S_n \times A$ are permutations of the Cartesian product set $\mathbb{Z}_n \times \mathbb{Z}_n$.

Proof. Since the n^2 entries of the juxtaposition $R_n \times A$ are exactly the n^2 elements of the set $\mathbb{Z}_n \times \mathbb{Z}_n$, then the entries

$$(i, a_{i0}), \quad (i, a_{i1}), \quad \ldots, \quad (i, a_{i(n-1)}),$$

of the ith row in $R_n \times A$ are distinct. This means that the ith row of A is a permutation of $\mathbb{Z}_n$. Similarly, the jth column of A is a permutation of $\mathbb{Z}_n$. Thus A is a Latin square.

Definition 4.5. Two Latin squares A and B based on $\mathbb{Z}_n$ are said to be *orthogonal* if their juxtaposition $A \times B$ is a permutation of the product set $\mathbb{Z}_n \times \mathbb{Z}_n$.

Example 4.2. The following two Latin squares

$$\begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} 0 & 1 & 2 & 3 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \end{bmatrix}$$

of order 4 are orthogonal since their juxtaposition

$$\begin{bmatrix} (0,0) & (1,1) & (2,2) & (3,3) \\ (1,3) & (0,2) & (3,1) & (2,0) \\ (2,1) & (3,0) & (0,3) & (1,2) \\ (3,2) & (2,3) & (1,0) & (0,1) \end{bmatrix}$$

is a permutation of the product set $\mathbb{Z}_4 \times \mathbb{Z}_4$.

□

Let $A_1, A_2, \ldots, A_k$ be Latin squares of order n. They are said to be *mutually orthogonal* if the juxtaposition $A_i \times A_j$ of each pair A_i, A_j $(i \neq j)$ is orthogonal. We abbreviate mutually orthogonal Latin squares as *MOLS*.

Theorem 4.6. *Let p be a prime number. Then the p-by-p matrices*

$$L_p^1, \quad L_p^2, \quad \ldots, \quad L_p^{p-1}$$

are $p-1$ mutually orthogonal Latin squares of order p.

Proof. Let r and s be integers such that $1 \leq r < s \leq p-1$. For any $(i,j) \in \mathbb{Z}_p^2$, the system

$$\begin{cases} rx + y & \equiv & i \pmod{p} \\ sx + y & \equiv & j \pmod{p} \end{cases}$$

of linear equations over the field $\mathbb{Z}_p$ has a unique solution. This means that each (i,j) appears in the juxtaposition $L_p^r \times L_p^s$. So L_p^r and L_p^s are orthogonal. □

Example 4.3. Let $n = p^k$ be a prime power and let $\mathbb{F}_n$ be a finite field of n elements. We list the elements of $\mathbb{F}_n$ as

$$a_0 = 0, \quad a_1, \quad a_2, \quad \ldots, \quad a_{n-1}.$$

For each nonzero element $a \in \mathbb{F}_n$, let L_n^a be the n-by-n matrix whose (i,j) entry a_{ij} is defined by

$$a_{ij} = aa_i + a_j \quad (i, j = 0, 1, \ldots, n-1).$$

The matrix L_n^a is a Latin square of order n based on $\mathbb{F}_n$.

For each fixed i, the set

$$aa_i + \mathbb{F}_n = \{aa_i + a_0,\, aa_i + a_1,\, \ldots,\, aa_i + a_{n-1}\}$$

is a translate of $\mathbb{F}_n$. Since $\mathbb{F}_n = aa_i + \mathbb{F}_n$, the ith row of L_n^a is a permutation of $\mathbb{F}_n$. For each fixed j, the set

$$a\mathbb{F}_n + a_j = \{aa_0 + a_j,\, aa_1 + a_j,\, \ldots,\, aa_{n-1} + a_j\}$$

is a translate of $a\mathbb{F}_n$. Since $\mathbb{F}_n = a\mathbb{F}_n$, the jth column of L_n^a is a permutation of $\mathbb{F}_n$. Thus L_n^a is a Latin square.

Theorem 4.7. *Let $n = p^k$ be a prime power and let $\mathbb{F}_n$ be a finite field of n elements. Then the Latin squares L_n^a $(a \in \mathbb{F}_n^*)$ of order n (based on $\mathbb{F}_n$) are mutually orthogonal.*

Proof. Let $a, b \in \mathbb{F}_n$ be distinct nonzero elements. We need to show that the Latin squares L_n^a and L_n^b are orthogonal. For any $(c, d) \in \mathbb{F}_n^2$, the system of linear equations

$$\begin{cases} ax + y &= c \\ bx + y &= d \end{cases}$$

over the finite field $\mathbb{F}_n$ has the unique solution $x = \frac{c-d}{a-b}$, $y = \frac{ad-bc}{a-b}$. This means that the (x, y) entry of L_n^a is $ax + y$, the (x, y) entry of L_n^b is $bx + y$, and the (x, y) entry of the juxtaposition $L_n^a \times L_n^b$ is $(ax + y, bx + y) = (c, d)$. We have seen that L_n^a and L_n^b are orthogonal. □

Example 4.4. Let $\mathbb{F}_4 = \{0, 1, \alpha, \alpha + 1\} = \mathbb{Z}_2[\alpha]/(\alpha^2 + \alpha + 1)$. Then

$$\begin{aligned}
L_4^1 &= \begin{bmatrix} 0 & 1 & \alpha & \alpha+1 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \end{bmatrix}, \\
L_4^\alpha &= \begin{bmatrix} 0 & 1 & \alpha & \alpha+1 \\ \alpha & \alpha+1 & 0 & 1 \\ \alpha+1 & \alpha & 1 & 0 \\ 1 & 0 & \alpha+1 & \alpha \end{bmatrix}, \\
L_4^{\alpha+1} &= \begin{bmatrix} 0 & 1 & \alpha & \alpha+1 \\ \alpha+1 & \alpha & 1 & 0 \\ 1 & 0 & \alpha+1 & \alpha \\ \alpha & \alpha+1 & 0 & 1 \end{bmatrix}
\end{aligned}$$

are mutually orthogonal Latin squares of order 4.

Theorem 4.8. *Let $A_1, A_2, \ldots, A_k$ be k mutually orthogonal Latin squares of order n. Then $k \leq n-1$, i.e., there are at most $n-1$ mutually orthogonal Latin squares of order n.*

Proof. Without loss of generality we may assume that each of the given Latin squares is based on $\mathbb{Z}_n$. Since switching the positions of one number with the positions of any other number in each of the Latin squares does not change the orthogonality, we may also assume that the given Latin squares are in standard form. Thus for each pair A_i, A_j $(i \neq j)$, the top row of the juxtaposition $A_i \times A_j$ is

$$[(0,0),(1,1),(2,2),\ldots,(n-1,n-1)].$$

Now consider the $(1,0)$-entry $a_{10}^{(i)}$ of each A_i $(1 \leq i \leq k)$. Since $a_{00}^{(i)} = 0$, we have $a_{10}^{(i)} \in \{1,2,\ldots,n-1\}$. We claim that $a_{10}^{(1)}, a_{10}^{(2)}, \ldots, a_{10}^{(k)}$ are distinct. Suppose $a_{10}^{(i)} = a_{10}^{(j)} = a$ $(i \neq j)$, then the $(1,0)$-entry of $A_i \times A_j$ is (a,a), which appears already in the top row of $A_i \times A_j$; this is contradictory to the orthogonality of A_i and A_j. Thus the distinctive property implies that $k \leq n-1$. □

For any integer $n \geq 2$, let $N(n)$ denote the largest number of mutually orthogonal Latin squares of order n. The first a few such numbers are

$$N(2)=1, \quad N(3)=2, \quad N(4)=3, \quad N(5)=4, \quad N(6)=1.$$

There do not exist two orthogonal Latin squares of order 6. If $n = p^k$ is a prime power, it has been shown in Theorem 4.7 that

$$N(p^k) = p^k - 1.$$

Theorem 4.9. *For each odd integer n, there exists a pair of mutually orthogonal Latin squares of order n, i.e., $N(n) \geq 2$ if n is odd.*

Proof. Let A be the matrix whose (i,j)-entry a_{ij} is

$$a_{ij} = i + j \pmod{n},$$

and let B be the matrix whose (i,j) entry b_{ij} is

$$b_{ij} = i - j \pmod{n}.$$

Since 1 and -1 is always invertible modulo n, the matrices A and B are Latin squares. We show that they are orthogonal. For each $(k,l) \in \mathbb{Z}_n$, since 2 is invertible modulo n, the linear system

$$\begin{cases} x+y &= k \\ x-y &= l \end{cases}$$

has the unique solution $x = \frac{k+l}{2}$, $y = \frac{k-l}{2}$. This means that each element of $\mathbb{Z}_n^2$ appears in the juxtaposition $A \times B$. So A and B are orthogonal. □

Let $A = [a_{ij}]$ be a Latin square of order m and let $B = [b_{kl}]$ a Latin square of order n. We construct a Latin square $A \otimes B$ of order mn as follows: For each (i, j)-entry a_{ij} of A , let $a_{ij} \otimes B$ be the n-by-n matrix

$$a_{ij} \otimes B = \begin{bmatrix} (a_{ij}, b_{11}) & (a_{ij}, b_{12}) & \cdots & (a_{ij}, b_{1n}) \\ (a_{ij}, b_{21}) & (a_{ij}, b_{22}) & \cdots & (a_{ij}, b_{2n}) \\ \vdots & \vdots & \ddots & \vdots \\ (a_{ij}, b_{n1}) & (a_{ij}, b_{n2}) & \cdots & (a_{ij}, b_{nn}) \end{bmatrix},$$

and for each (k, l)-entry b_{jk} of B, let $A \otimes b_{kl}$ be the m-by-m matrix

$$A \otimes b_{kl} = \begin{bmatrix} (a_{11}, b_{kl}) & (a_{12}, b_{kl}) & \cdots & (a_{1m}, b_{kl}) \\ (a_{21}, b_{kl}) & (a_{22}, b_{kl}) & \cdots & (a_{2m}, b_{kl}) \\ \vdots & \vdots & \ddots & \vdots \\ (a_{m1}, b_{kl}) & (a_{m2}, b_{kl}) & \cdots & (a_{mm}, b_{kl}) \end{bmatrix}.$$

The mn-by-mn matrix $A \otimes B$, written in block matrix form, is defined as

$$A \otimes B = \begin{bmatrix} a_{11} \otimes B & a_{12} \otimes B & \cdots & a_{1m} \otimes B \\ a_{21} \otimes B & a_{22} \otimes B & \cdots & a_{2m} \otimes B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} \otimes B & a_{m2} \otimes B & \cdots & a_{mm} \otimes B \end{bmatrix} = \begin{bmatrix} A \otimes b_{11} & A \otimes b_{12} & \cdots & A \otimes b \\ A \otimes b_{21} & A \otimes b_{22} & \cdots & A \otimes b \\ \vdots & \vdots & \ddots & \vdots \\ A \otimes b_{n1} & A \otimes b_{n2} & \cdots & A \otimes b \end{bmatrix}$$

Proposition 4.10. *Let A_1 and A_2 be orthogonal Latin squares based on $\mathbb{Z}_m$. Let B_1 and B_2 are orthogonal squares based on $\mathbb{Z}_n$. Then the matrices $A_1 \otimes B_1$ and $A_2 \otimes B_2$ are orthogonal Latin squares based on $\mathbb{Z}_m \times \mathbb{Z}_n$.*

Proof. We identify the set $\mathbb{Z}_m \times \mathbb{Z}_n$ with the set $\mathbb{Z}_{mn}$ by the map $(i, k) \mapsto in + k$, i.e.,

$$\begin{array}{rclrclcr} (0,0) & \mapsto & 0, & (0,1) & \mapsto & 0, & \ldots, & (0, n-1 \\ (1,0) & \mapsto & n, & (1,1) & \mapsto & n+1 & \ldots, & (1, n-1 \\ & \vdots & & & \vdots & & & \\ (m-1,0) & \mapsto & (m-1)n, & (m-1,1) & \mapsto & (m-1)n+1 & \ldots, & (m-1, n-1 \end{array}$$

Let $A = [a_{ij}]$ and $B = [b_{kl}]$ be Latin squares of order m and n respectively. For each $s \in \mathbb{Z}_{mn}$, let $s = in + k$, where $0 \leq i \leq m-1$ and $0 \leq k \leq n-1$. The sth row of $A \otimes B$ is

$$\big[(a_{i0}, b_{k0}),\ (a_{i0}, b_{k1}),\ \ldots,\ (a_{i0}, b_{k(n-1)});\quad (a_{i1}, b_{k0}),\ (a_{i1}, b_{k1}),\ \ldots,\ (a_{i1}, b_{k(n-1)});$$
$$\ldots;\quad (a_{i(m-1)}, b_{k0}),\ (a_{i(m-1)}, b_{k1}),\ \ldots,\ (a_{i(m-1)}, b_{k(n-1}$$

which is converted into the row

$$\big[a_{i0}n + b_{k0},\ a_{i0}n + b_{k1},\ \ldots,\ a_{i0}n + b_{k(n-1)};\quad a_{i1}n + b_{k0},\ a_{i1}n + b_{k1},\ \ldots,\ a_{i1}n +$$
$$\ldots;\quad a_{i(m-1)}n + b_{k0},\ a_{i(m-1)}n + b_{k1},\ \ldots,\ a_{i(m-1)}$$

It is clear that for each j $(0 \leq j \leq m-1)$ the numbers

$$a_{ij}n + b_{k0}, \quad a_{ij}n + b_{k1}, \quad \ldots, \quad a_{ij}n + b_{k(n-1)}$$

are distinct. If $a_{ij}n + b_{kt} = a_{ij'} + b_{kt'}$, where $j \neq j'$ and $t \neq t'$, then $(a_{ij} - a_{ij'})n = b_{kt'} - b_{kt}$. Since $0 \leq b_{kt} \leq n-1$ and $0 \leq b_{kt'} \leq n-1$, it follows that $b_{st} = b_{st'}$ and $a_{ij} = a_{ij'}$. Thus $t = t'$ and $j = j'$. This means that the sth row of $A \otimes B$ is a permutation of $\mathbb{Z}_{mn}$. Similarly, the sth column of $A \otimes B$ is also a permutation of $\mathbb{Z}_{mn}$. Hence the matrix $A \otimes B$ is a Latin square of order mn.

To prove $A_1 \otimes B_1$ and $A_2 \otimes B_2$ to be orthogonal, consider an arbitrary ordered pair $(s, t) \in \mathbb{Z}_{mn}^2$. There are unique integers i, k and j, l such that

$$s = in + k \quad \text{and} \quad t = jn + l,$$

where $0 \leq i, j \leq m-1$ and $0 \leq k, l \leq n-1$. Then (i, j) is an entry of $A_1 \otimes B_1$, (k, l) is an entry of $A_2 \otimes B_2$, and

$$((i, k), (j, l)) \mapsto (in + k, jn + l) = (s, t).$$

This means that each entry $(s, t) \in \mathbb{Z}_{mn}^2$ appears in the juxtaposition $(A_1 \otimes B_1) \times (A_2 \otimes B_2)$. So $A_1 \otimes B_1$ and $A_2 \otimes B_2$ are orthogonal. □

Example 4.5. The matrices

$$A_1 = \begin{bmatrix} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{bmatrix} \quad \text{and} \quad A_2 = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 0 & 2 \\ 2 & 1 & 0 \end{bmatrix}.$$

are orthogonal Latin squares of order 3. The matrices

$$B_1 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \end{bmatrix} \quad \text{and} \quad B_2 = \begin{bmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{bmatrix}$$

are orthogonal Latin squares. Then $A_1 \otimes B_1$ is the Latin square

$$A_1 \otimes B_1 = \begin{bmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 1 & 0 & 3 & 2 & 5 & 4 & 7 & 6 & 9 & 8 & 11 & 10 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 & 10 & 11 & 8 & 9 \end{bmatrix}.$$