Sets of Orthogonal Latin Squares

To obtain sets of $p-1$ mutually orthogonal Latin Squares (MOLS) of side p where p is prime or a power of a prime, we associate each of the treaments with an element of the Galois Field of $p = s^n$ elements (i.e.$GF(s^n)$) in a 1 to 1 correspondence.

Galois Fields

The set $\{g_o, g_1, ..., g_{p-1}\}$of p elements is a finite field of order p if:

1. Addition:

- **a**. $g_i + g_j = g_j + g_i$
- **b**. $g_i + (g_j + g_k) = (g_i + g_j) + g_k$
- **c**. Given g_i and g_k $\exists!\ g_j \ni \cdot\ g_i + g_j = g_k$
- **d**. the element having trhe additive propoerty of zero is $g_o \ni \cdot\ g_j + g_0 = g_j\ \forall j$

2. Multiplication:

- **a**. $g_i g_j = g_j g_i$
- **b**. $g_i(g_j g_k) = (g_i g_j)g_k$
- **c**. $g_i(g_j + g_k) = g_i g_j + g_i g_k$
- **d**. Given any $g_i (\neq g_0)$ and any g_k $\exists!\ g_j \ni \cdot\ g_i g_j = g_k$ and g_0 has the multiplicative property of zero i.e.$g_0 g_i = g_0$
- **e**. The element having the multiplicative property of unity is g_1.

Case 1: If p is a prime.

The finite field of p elements is represented by $g_0 = 0, g_1 = 1, g_i = i, i = 2, ..., p-1$.
Addition and multiplication are ordinary arithmetic operations, except the resulting number is reduced *mod p*.

Case 2: Galois Field of $p = s^n$ elements where s is a prime

Let $P(x)$ be an irreducible polynomial of degree n with integer coefficients.

i.e. $P(x) \neq P_1(x)P_2(x) + sP_3(x)$ where $P_1,\ P_2$ and P_3 are polynomials (with integer coefficients) of degrees less than n.

For any polynomial $F(x),$ a polynomial in x with integer coefficients). then

$$F(x) = f(x) \quad mod\ (s, P(x))$$

i.e. this means we can write

$$F(x) = sq(x) + P(x)Q(x) + f(x)$$

and

$$f(x) = a_0 + a_1x^1 + a_2x^2 + ... + a_{n-1}x^{n-1}$$

is the "*residue*" of $F(x)\ \ mod(s, P(x))$ and $a_o, ..., a_{n-1} \varepsilon \{0, 1, ..., s-1\}$.

If s and $P(x)$ are fixed and $f(x)$ varies, we get s^n classes formed since a_i takes s values. (Note: In order that division be unique, s must be prime and $P(x)$ irreducible *mod s*).

The finite field formed by the s^nclasses of residues $f(x)$ is called $GF(s^n)$ (i.e. Galois Field of s^n) and the s^n classes are the same regardless of the choice of $P(x)$, as long as $P(x)$ is irreducible.

$GF(s^n)$ exists if s is prime and n is a positive integer. The classes of residues may be represented by the different possible $f_i(x)$. We denote them by $g_0, g_1, ..., g_{p-1}$.

We generally represent the elements of $GF(p)$ as *powers of an element y* (called the ***primitive mark*** or P.M.) of the field such that $y^{p-1} = 1$ and this is the smallest power for which this is true.

i.e. elements are $g_o = 0, g = 1, g_2 = y, ..., g_{p-1} = y^{p-2}$

Then the addition table forms a L.S.D. and other squares are obtained by cyclically rotating all rows but the first.

e.g. $p = 4(p = s^n$ so $s = 2, n = 2)$

$GF(p = s^n)$ is $GF(4 = s^2)$ here. Its elements are $g_0 = 0, g_1 = 1, g_2 = x$(=the primitive mark y) and $g_3 = y^2 = 1 + x$

Arithmetic is carried out *mod* 2 and $y = x$ is P.M.

The irreducible polynomial $P(x)$ of degree 2 in the field is $P(x) = x^2 + x + 1$(it is irreducible $mod\ s = 2$). Now we can write that

$f_1(x) = a_0 + a_1x$ where $a_0, a_1 \varepsilon \{0, , 1\}$ so

$$f(x) = \begin{cases} 0 \\ 1 \\ x \\ 1+x \end{cases}$$

The P.M. is such that $y^{p-1} = (f(x))^{p-1} = 1$ and $p = 4$

Note: If $y = x$: then we have $y^3 = x^3 = 1 \bmod (P(x), s)$ so $y = x$

If we had set $y = 1 + x$: then we have that

$$\begin{aligned} y^3 &= (1+x)^3 \\ &= y^2 y \end{aligned}$$

and one lower power $\neq 1$

i.e. $x^2 = (x^2 + x + 1) - (1 + x) = 1 + x \bmod(s, P(x))$

Note: $g_4 = y^3 = y^2 y = (1+x)x = x^2 + x = (x^2 + x + 1) - 1 = -1 = +1 \bmod(s, P(x))$

In the addition table, the first row consists of the elements $0, 1, x, 1+x$ and the table becomes

	0	1	x	$1+x$
then add (1)	1	0	$1+x$	x
then add (x)	x	$1+x$	0	1
then add ($1+x$)	$1+x$	x	1	0

Writing A,B,C,D for the elements $0, 1, x, 1+x$ respectively, and rotating all but the first row cyclically we get

A	B	C	D
B	A	D	C
C	D	A	B
D	C	B	A

A	B	C	D
C	D	A	B
D	C	B	A
B	A	D	C

A	B	C	D
D	C	B	A
B	A	D	C
C	D	A	B

i.e. 3 MOLS of side $p = 4$.

Construction of L.S. and MOLS

Theorem: $\exists$ a set of p-1 mutually orthogonal Latin Squares (MOLS) of side p where $p = s^n$(p is prime or a power of a prime). We associate each of the treatments with an element of $GF(p = s^n)$ in a 1-1 correspondence. Elements of the field are ordered as $g_0 = 0, g_1 = 1, g_2 = y, ..., g_{p-1} = y^{p-2}$ where y is a primitive mark (P.M.) of the field. (i.e.$y^{p-1} = 1$ and no lower power $y^q = 1$ for $0 < q < p$). The additive table forms a L.S. and other squares are obtained by rotating cyclically all rows but the first.

Theorem: The i^{th} square of a set of $p-1$ MOLS has $g_i = x^{i-1}$ as the first element of the second row. The first element of the $(m+1)^{st}$ row is $g_i y^{m-1} = g_i g_m$

Therefore the i^{th} square is

g_0	g_1	$\cdots$	g_{p-1}
g_i	$g_1 + g_i$	$\cdots$	$g_{p-1} + g_i$
$g_i g_2$	$g_i + g_i g_2$	$\cdots$	$g_{p-1} + g_i g_2$
$\vdots$	$\vdots$	$\cdots$	$\vdots$
$g_i g_{p-1}$	$g_i + g_i g_{p-1}$	$\cdots$	$g_{p-1i} + g_i g_{p-1}$

Note:A typical element is $g_i g_j + g_l$ where $i = 1, ..., p-1; j = 0, 1, ..., p-1; l = 0, 1, ..., p-1$

Theorem: Such a square is a Latin Square

Proof: (by contradiction)
Suppose it is not a Latin square and therefore that 2 elements in $(q+1)^{th}$row (say) are identical.
i.e. For some pair t, u, $(t \neq u)$

$$g_i g_q + g_t = g_i g_q + g_u$$

Then $g_t = g_u \quad (t \neq u)$
Contradiction! (since the elements of the field are distinct)

Do the same for columns:

$$g_i g_q + g_t = g_i g_l + g_t \qquad (q \neq l)$$

so

$$g_i(g_q - g_l) = 0$$

which implies $g_q = g_l$ since $g_{ii} \neq 0$.
Contradiction!

Theorem: The squares in the set are mutually orthogonal.

Proof: (by contradiction)
Suppose squares i and j are not orthogonal.
Therefore when j^{th} is superimposed on i^{th} , at least 2 cells are the same. (i.e. one pair of elements occurs together in two of the cells)
Suppose (w.l.o.g) in $(q+1)^{th}$row, $(t+1)^{th}$ column and $(r+1)^{th}$ row, $(y+1)^{th}$ column, where $q \neq r, t \neq y$

Elements of i^{th}square coincide:(Latin letters equal)

$$g_i g_q + g_t = g_i g_r + g_u$$

Elements of jthsquare coincide:(Greek letters equal)

$$g_j g_q + g_t = g_j g_r + g_t$$

or

$$(g_i - g_j) g_q = (g_i - g_j) g_r$$

$\Rightarrow$

$$g_i = g_j$$

or

$$g_q = g_r$$

Contradiction!

Table of $P(x)'s$ and P.M.'s

s^n	$P(x)$	P.M.
2^2	x^2+x+1	x
2^3	x^3+x^2+1	x
2^4	x^4+x+1	$1+x$
3^2	x^2+1	$1+x$
3^3	x^3+2x+1	x
5^2	x^2+x+1	$2+x$

Analysis of Several Latin Squares

Running MOLS allows us to get more d.f. for error and to conduct more hypothesis tests.
Consider the model

$$y_{hijk} = \mu + \pi_h + \rho_{i(h)} + \gamma_{j(h)} + \tau_k + (\pi\tau)_{hk} + \varepsilon_{hijk}$$

where h =square, i =row, j =column, k =treatment

Impose side conditions:
$\sum_h \pi_h = 0; \sum_k \tau_k = 0;$ and for each h $\sum_i \rho_{i(h)} = 0; \sum_j \gamma_{j(h)} = 0; \sum_k (\pi\tau)_{hk} = 0;$ and for each k $\sum_h (\pi\tau)_{hk} = 0$

Suppose we have squares each of side p therefore $i, j, k = 1, \ldots, p; h = 1, \ldots, s$

The solutions to the N.E.'s are:

$$\hat{\mu} = \bar{y}_{....}$$

$$\hat{\pi}_h = \bar{y}_{h...} - \bar{y}_{....}$$

$$\hat{\tau}_k = \bar{y}_{...k} - \bar{y}_{....}$$

Holding h fixed,

$$\hat{\rho}_{i(h)} = \bar{y}_{hi..} - \bar{y}_{h...}$$

;

$$\hat{\gamma}_{j(h)} = \bar{y}_{h.j.} - \bar{y}_{h...}$$

;

$$\begin{aligned}(\pi\tau)_{hk} &= (\bar{y}_{h..k} - \bar{y}_{....}) - (\bar{y}_{h...} - \bar{y}_{....}) - (\bar{y}_{...k} - \bar{y}_{....}) \\ &= \bar{y}_{h..k} - \bar{y}_{h...} - \bar{y}_{...k} + \bar{y}_{....}\end{aligned}$$

ANOVA table

Source of Variation	**d.f.**	**S.S.**
Total	$sp^2 - 1$	$\sum_h \sum_i \sum_j \sum_k y_{hijk}^2 - C.. = T.S.S.$
Squares (S)	$s - 1$	$\sum_{h=1}^{s} \frac{T_{h\cdots}^2}{p^2} - C.M. = S_S$
Treatments (T)	$p - 1$	$\sum_{k=1}^{p} \frac{T_{\cdots k}^2}{p^2} - C.M. = S_T$
T x S interaction	$(s-1)(p-1)$	$\sum_{h=1}^{s} \sum_{k=1}^{p} \frac{T_{h\cdot\cdot k}^2}{p^2} - C.M. - S_T - S_S$
Rows in squares	$s(p-1)$	$\sum_h \left(\sum_{s=1}^{p} \frac{T_{hi\cdot\cdot}^2}{p} - \frac{T_{h\cdots}^2}{p^2} \right)$
Columns in squares	$s(p-1)$	$\sum_h \left(\sum_{j=1}^{p} \frac{T_{h\cdot j\cdot}^2}{p} - \frac{T_{h\cdots}^2}{p^2} \right)$
Error	$s(p-1)(p-2)$	by subtraction

Randomization for Latin Squares:

Select a random square. Assign rows, columns, and treatments at random in each square. Do this for each of the *s* squares.