ORTHOGONAL LATIN SQUARES

AND

INCOMPLETE BALANCED BLOCK DESIGNS

ORTHOGONAL LATIN SQUARES
AND
INCOMPLETE BALANCED BLOCK DESIGNS

By

PETER BEDROSIAN, B.A.

A Thesis

Submitted to the Faculty of Arts and Science

in Partial Fulfilment of the Requirements

For the Degree

Master of Arts

McMaster University

October 1953

MASTER OF ARTS (1953) McMASTER UNIVERSITY
(Mathematics) Hamilton, Ontario

TITLE: Orthogonal Latin Squares and Incomplete Balanced Block Designs

AUTHOR: Peter Bedrosian, B.A. (McMaster University)

SUPERVISOR: Professor J.D. Bankier

NUMBER OF PAGES: 132

SCOPE AND CONTENTS:

Methods of constructing orthogonal Latin squares and incomplete balanced block designs are developed. The analysis of these designs is then derived. Particular care is taken in the determination of the number of degrees of freedom involved, a point which is usually neglected in other sources. The principle source of material for this thesis has been H.B. Mann's book, Analysis and Design of Experiments.

TABLE OF CONTENTS

CHAPTER I

GALOIS FIELDS AND ORTHOGONAL LATIN SQUARES

A Latin square of side m is an arrangement of m letters into m^2 subsquares of a square in such a way that every row and every column contains every letter exactly once. If one takes two Latin squares of the same dimension and superimposes one upon the other, and finds that no ordered pair of letters are the same, then the two Latin squares are termed orthogonal. The following Latin squares

A	B	C	α	β	γ
B	C	A	γ	α	β
C	A	B	β	γ	α

are orthogonal. In this chapter we will consider methods for constructing orthogonal Latin squares.

In order to fully comprehend the methods of constructing Latin squares certain concepts of algebra and the theory of numbers must be known.

Let a, b and m be integers. We say that a is congruent to b modulo m, $a \equiv b(m)$, if m divides a-b. We will make use of the following properties of congruences.

(1) If $a \equiv b(m)$, then $a \pm c \equiv b \pm c(m)$, $ac \equiv bc(m)$.

(2) If $ac \equiv bc(m)$ and $(m,c) = t$ then $a \equiv b(\frac{m}{t})$.[1]

---

[1] Uspensky and Heaslet, Elementary Number Theory. New York: McGraw-Hill, 1939, pp. 128-133.

In the following work we shall always consider the least positive residue modulo p, that is, we replace each number by the remainder, r, obtained by division by p, where $0 \leq r < p$.

Form the following pattern where p is a prime

$$L_j = \begin{array}{llll} 0 & 1 & \dots & p-1 \\ j & 1+j & \dots & p-1+j \\ 2j & 1+2j & \dots & p-1+2j \\ \vdots & \vdots & & \vdots \\ (p-1)j & 1+(p-1)j & \dots & (p-1)+(p-1)j \end{array} \qquad j = 1,2,\dots,p-1.$$

All the numbers in L_j are the least positive residues modulo p. We shall show that L_j is a Latin square. Suppose L_j were not a Latin square. Then in some row or column a number would appear twice. Consider the ith row as being such a row where the element in the rth column is the same as the element in the kth column. Thus $(k-1)+(i-1)j \equiv (r-1)+(i-1)j \ (p)$. From this relationship $k \equiv r \ (p)$. Then since $0 < k,r \leq p$, $k = r$. Similarly we can show that every column contains every number only once. Thus L_j $(j = 1,2, \dots,p)$ is a Latin square.

We shall show next that L_i is orthogonal to L_j if $i \neq j$. Assume that L_i is a Latin square which is not orthogonal to L_j. Then there would be two cells in which the ordered pair of numbers would be the same. Suppose mn is the pair that occurs twice. Suppose also that it occurs in the αth row and βth column and the γth row and δth column. Then

$$\beta + \alpha j \equiv \delta + \gamma j \equiv m \ (p),$$

$$\beta+\alpha i \equiv \delta+\gamma i \equiv n\ (p).$$

Hence $\alpha(i-j)\equiv\gamma(i-j)$ (p). But $|i-j| < p$ and thus $(i-j,p)=1$. By the rule of division of congruences we may divide by $(i-j)$. We obtain $\alpha\equiv\gamma$ (p), $\beta\equiv\delta$ (p), and hence $\alpha=\gamma$, $\beta=\delta$. This is a contradiction. Hence L_i is orthogonal to L_j.

A set of four orthogonal five-sided squares is presented as an example:

L_1	L_2	L_3	L_4
0 1 2 3 4	0 1 2 3 4	0 1 2 3 4	0 1 2 3 4
1 2 3 4 0	2 3 4 0 1	3 4 0 1 2	4 0 1 2 3
2 3 4 0 1	4 0 1 2 3	1 2 3 4 0	3 4 0 1 2
3 4 0 1 2	1 2 3 4 0	4 0 1 2 3	2 3 4 0 1
4 0 1 2 3	3 4 0 1 2	2 3 4 0 1	1 2 3 4 0.

Note in particular that the uniqueness of division was necessary in constructing L_j. Because of this unique characteristic the residues $\underline{a}, 2\underline{a}, \ldots, (p-1)\underline{a}$ are (p-1) different residues all different from zero provided that $a\not\equiv 0$ (p). Thus one of these residues must be 1. Accordingly, corresponding to every residue $\underline{a}\not\equiv 0$ (p) there exists a residue a^{-1} called the inverse of $\underline{a}$ such that $a^{-1}a\equiv 1$ (p).

The method presented for constructing m-1 orthogonal Latin squares if m is a prime suggests that m-1 orthogonal Latin squares may be constructed if we have a field F consisting of m elements which satisfy the following conditions.

For every pair of elements $\underline{a}$, b in F, there exist two uniquely determined elements $\underline{a}+b$ and $\underline{a}b$ in F. The "addition"

and "multiplication" have the following properties.

I The commutative law holds,

$$a+b=b+a,\quad ab=ba.$$

II The associative law holds,

$$(a+b)+c=a+(b+c),\quad (ab)c=a(bc).$$

III There exist two elements 0, 1 in F such that $a+0=a$ and $a1=a$ for every a in F.

IV Corresponding to every $a\neq 0$ there exists an element $(-a)$ and an element a^{-1} such that

$$a+(-a)=0 \text{ and } aa^{-1}=1.$$

The element a^{-1} is called the inverse of a.

V The distributive law holds,

$$c(a+b)=ca+cb.$$

Any system satisfying the above postulates is called a field. When the number of elements (which are also referred to as the marks of the field) is finite, then the field is known as a finite field or Galois field (G.F.).

Let $g_0=0$, $g_1=1$, g_2, ..., g_{m-1} be the elements of the finite field and form the following pattern which forms an addition table for the G.F.(p^m) since the elements in the first column are all the elements of the field.

$$L_i=\begin{matrix} 0 & 1 & \cdots & g_{m-1} \\ g_i & g_i+1 & \cdots & g_i+g_{m-1} \\ g_ig_2 & g_ig_2+1 & \cdots & g_ig_2+g_{m-1} \\ \vdots & \vdots & & \vdots \\ g_ig_{m-1} & g_ig_{m-1}+1 & \cdots & g_ig_{m-1}+g_{m-1}. \end{matrix} \quad (i=1, \ldots, m-1) \tag{1.1}$$

We have here a set of m-1 orthogonal Latin squares. For, if L_i is not a Latin square, then one column, say the p th column, would contain the same number twice, once in the kth row and once in the rth row. Thus we should have

$$g_i g_{k-1} + g_{p-1} = g_i g_{r-1} + g_{p-1} ,$$

$$g_i g_{k-1} = g_i g_{r-1} .$$

Since $g_i \neq 0$ and every non-zero element in a field has an inverse, then

$$g_i^{-1} g_i g_{k-1} = g_i^{-1} g_i g_{r-1} ,$$

and $g_{k-1} = g_{r-1}$. Thus $k = r$. By a similar argument we can show that each row contains every number exactly once. We can now say that L_i , $(i = 1, 2, \ldots, m-1)$ is a Latin square. Now it must be shown that L_j is orthogonal to L_i if $i \neq j$. If this were not so then we should have the same ordered pair of numbers occuring in two different cells of the square formed by superimposing L_i upon L_j. Let the pair which occurs twice be in the αth row and δth column. Then

$$g_i g_{\alpha-1} + g_{\beta-1} = g_i g_{\gamma-1} + g_{\delta-1} ,$$

$$g_j g_{\alpha-1} + g_{\beta-1} = g_j g_{\gamma-1} + g_{\delta-1} .$$

By subtraction

$$g_{\alpha-1}(g_j - g_i) = g_{\gamma-1}(g_j - g_i) .$$

Since $g_i \neq g_j$, $(g_j - g_i)^{-1}$ exists, and $g_{\alpha-1} = g_{\gamma-1}$. Hence $\alpha = \gamma$. Substituting in the first equation we see that $\beta = \delta$. Thus we have proved the following theorem.

Theorem 1.1: If $g_0 = 0$, $g_1 = 1$, g_2, ..., g_{m-1} are the marks of a finite field, then the designs L_i of (1.1) form a set of m-1

orthogonal Latin squares.

The following propositions are valid over a field F.

Proposition 1: $\underline{a}.0 = 0$ for every $\underline{a}$.

Proof: We have $a = a(1+0) = a + a0$. If we add $(-a)$ to both sides of this equation, we obtain Proposition 1.

Proposition 2: $ab = 0$, $a \neq 0$ implies $b = o$.

Proof: This follows by multiplying $ab = 0$ by a^{-1} on the left.

We denote by $m.x$, where m is a positive integer and x is a mark of F, the sum of m x's.

Proposition 3: If m is an integer, such that $m.1 = 0$, then $m.x = 0$ for all x in F. If $m.x = 0$ for one $x \neq 0$, then $m.y = 0$ for all y in F.

Proof: If $m.1 = 0$ then $m.x = (m.1)x = 0x = 0$. Also if $m.x = 0$ then $m.x = (m.1)x = 0$. If $x \neq 0$ then, by Proposition 1, $m.1 = 0$ and therefore $m.y = 0$ for every y.

Proposition 4: If p is the smallest positive integer for which $p.1 = 0$ then p is a prime.

Proof: Suppose $p = mn$, $0 < m, n < p$, then $(m.n).1 = m.(n.1) = 0$. Hence if $n.1 = 0$ then we get a contradiction, because $n < p$. By Proposition 3 if $n.1 \neq 0$, then $m.y = 0$ for all y in F. In particular $m.1 = 0$, which is impossible. Hence p is a prime.

The number p is called the characteristic of the field. If there is no integer p for which $p.1 = 0$ then the field is called a field of characteristic zero and is necessarily infinite because the elements $n.1$, $n = 0,1,2, \ldots$, are then all different.

Any positive integer m may be written in the form $m = a + \lambda p$, $0 \leq a \leq p-1$, where λ is a non-negative integer. Then

$$m.x = (a + \lambda p).x = a.x$$

for any element x of F by Proposition 3. Thus we may replace m by its least positive residue modulo p in such calculations and we shall do so in the proof of the next theorem. We shall also rename certain elements in F using $\underline{a}$ to represent either a non-negative integer or the element of F, $a.1$, $0 \leq a \leq p-1$. Then we may write

$$a.x = (a.1)x = ax.$$

This should not lead to confusion in the work that follows.

Theorem 1.2: The number of elements in a Galois field F is a power of its characteristic p.

Proof: Put $w_1 = 1$. If there is a mark $w_2 \neq a.1 = a$ for $a = 0, 1, \ldots, p-1$ form the marks $a_1w_1 + a_2w_2$ and form all the marks $a_1w_1 + a_2w_2 + a_3w_3$. Continue this process until all the marks of F are exhausted. If $w_1, \ldots, w_m$ are obtained in this way, then $a_1w_1 + \ldots + a_mw_m, (a_i = 0, 1, \ldots, p-1)$, represent all the marks of F and are p^m in number. For, if

$$a_1w_1 + \ldots + a_mw_m = b_1w_1 + \ldots + b_mw_m ,$$

then $(a_1-b_1).w_1 + \ldots + (a_m-b_m).w_m = 0$. Let k be the largest number for which $a_k - b_k = -c_k \neq 0$. Then

$$w_k = c_k^{-1}(a_1-b_1)w_1 + \ldots + c_k^{-1}(a_{k-1}-b_{k-1})w_{k-1}$$

$$= d_1w_1 + \ldots + d_{k-1}w_{k-1}$$

where $d_1, \ldots, d_{k-1}$ are residues modulo p. But this contradicts

the significance of w_k. Hence F contains p^m elements.

Let α be any mark of a Galois field, G.F.(p^m), and form $1, \alpha, \alpha^2, \ldots, \alpha^k, \ldots$. Since the number of marks is finite we must have, for some $k > j$,

$$\alpha^k = \alpha^j, \quad \alpha^{k-j} = 1.$$

Definition: The order, t, of any element, α, in a G.F.(p^m) is the least positive power to which that element must be raised to give the identity element of the field.

Let $x_1, \ldots, x_{p^m-1}$ be all the non-zero elements of the G.F.(p^m). Then

$$\alpha x_1 \alpha x_2 \cdots \alpha x_{p^m-1} = x_1 x_2 \cdots x_{p^m-1}$$

if $\alpha \neq 0$, since $\alpha x_i = \alpha x_j$ implies that $x_i = x_j$ and thus the elements αx_i, $i = 1, \ldots, p^m-1$, must all be distinct. Hence

$$\alpha^{p^m-1} = 1 \text{ for all } \alpha \neq 0.$$

We shall continue to prove several additional propositions on the order of elements in a finite field.

Proposition 5: If s is the order of α and $\alpha^n = 1$, then $n \equiv 0(s)$.

Proof: There exists an integer λ and r such that $n = \lambda s + r$, $0 \leq r < s$. Also $\alpha^n = 1$ implies $\alpha^t = 1$ since $\alpha^{\lambda s} = 1$. Hence $r = 0$, since $r < s$.

Corollary: If s is the order of α then $p^m - 1 \equiv 0$ (s).

Proposition 6: If α has the order s and β the order t and $(s,t) = 1$ then $\alpha\beta$ has the order st.

Proof: For any $r > 0$, if $(\alpha\beta)^r = 1$, then $(\alpha\beta)^{rs} = 1$ and hence $\beta^{sr} = 1$. Also $sr \equiv 0$ (t) by Proposition 5. Hence $r \equiv 0$ (t), since $(s,t) = 1$. Again, if $(\alpha\beta)^t = 1$, it follows that $\alpha^{tt} = 1$ and st

is thus the order of $\alpha\beta$.

Proposition 7: If α has the order $\lambda\mu$ then α^{λ} has the order μ.

Proof: Let the order of α^{λ} be s. Then $(\alpha^{\lambda})^{s} = 1$. Since $(\alpha^{\lambda})^{\mu} = 1$, $\mu \equiv 0(s)$ by Proposition 5. Since $\alpha^{\lambda s} = 1$ and the order of α is $\lambda\mu$, $\lambda s \equiv 0\ (\lambda\mu)$. From this it follows that $s \equiv 0\ (\mu)$ and $s = \mu$.

Proposition 8: If s is the largest order of any element in a Galois field F and t is the order of any element, then $s \equiv 0\ (t)$.

Proof: If $s \not\equiv 0\ (t)$ then for some prime $p > 0$, we would have $s = p^{e}r$, $t = p^{f}r'$, $(p,r) = (p,r') = 1$, $f > e$. For otherwise, every prime factor of t would occur in s to the same power or to a higher power and we would have $s \equiv 0\ (t)$. Now $\alpha^{p^{e}}$ is an element in the field F and has order r since $(\alpha^{p^{e}})^{r} = 1$ for if the order of $\alpha^{p^{e}}$ were $g < r$ then $\alpha^{p^{e}g} = 1$ and $p^{e}g < s$ which is impossible since s is the order of α. Similarly p^{f} is the order of $\beta^{r'}$ since $(\beta^{r'})^{p^{f}} = 1$. By Proposition 6 since $(p^{f},r) = 1$ then $\alpha^{p^{e}}\beta^{r'}$ has order $p^{f}r$. Since $f > e$ then $p^{f}r > s$ which is impossible. Thus our assumption is false. Therefore $s \equiv 0\ (t)$.

Definition: An element of order $p^{m}-1$ in the Galois field of order p^{m} is called a primitive root.

Lemma 1.1: A monic polynomial $P_{n}(x) = x^{n} + a_{1}x^{n-1} + \ldots + a_{n}$ of degree n with coefficients in G.F.(p^{m}) has at most n roots.

Now consider the polynomial $P_{n}(x)$ of degree n.

Case 1: $P_{n}(x)$ has no roots in G.F.(p^{n}).

Our assumption is true since $0 < n$.

Case 2: $P_{n}(x)$ has at least one root, α_{1}. Then $P_{n}(\alpha_{1}) = 0$.

Hence

$$P_n(x) = P_n(x) - P_n(\alpha_1)$$
$$= x^n - \alpha_1^n + a_1 x^{n-1} - a_1\alpha_1^{n-1} + \ldots + a_{n-1}(x-\alpha_1)$$
$$= (x-\alpha_1)Q(x)$$

where $Q(x)$ is a monic polynomial of degree n-1. By our induction assumption $Q(x)$ has at most n-1 roots and hence $P_n(x)$ may be written in the form

$$P_n(x) \equiv (x-\alpha_1)^{\ell_1}(x-\alpha_2)^{\ell_2}\ldots(x-\alpha_k)^{\ell_k}R(x),\ \alpha_i \neq \alpha_j,\ i \neq j,$$

where $\ell_1 + \ell_2 + \ldots + \ell_k \leq n$ and $R(x)$ has no roots in G.F.(p^n) and also where $R(x)$ is a monic polynomial of degree $n-(\ell_1 + \ell_2 + \ldots + \ell_k)$.

Suppose $P_n(x)$ has a root β different from α_i, $i = 1,2, \ldots, k$. Thus

$P_n(\beta) = 0 = (\beta-\alpha_1)^{\ell_1}(\beta-\alpha_2)^{\ell_2}\ldots(\beta-\alpha_k)^{\ell_k}R(\beta)$ where $R(\beta) \neq 0$. Hence β must be one of the α_i, $i = 1,2, \ldots, k$. But this is impossible by our hypothesis. Therefore the distinct roots of $P_n(x)$ are $\alpha_i, i = 1,2,\ldots,k$.

Suppose α_1 is a root of $P(x)$ of multiplicity $m_1 > \ell_1$. This means that

$$P(x) \equiv (x-\alpha_1)^{m_1}D(x) \text{ where } D(\alpha_1) \neq 0$$

and the degree of $D(x)$ is $n-m_1$. Hence

$$(x-\alpha_2)^{\ell_2}\ldots(x-\alpha_k)^{\ell_k}R(x) \equiv (x-\alpha_1)^{m_1-\ell_1}D(x).$$

Set $x = \alpha_1$. Then

$$(\alpha_1-\alpha_2)^{\ell_2}\ldots(\alpha_1-\alpha_k)^{\ell_k}R(\alpha_1) = 0.$$

Since $\alpha_i \neq \alpha_j$ for $i,j = 1,2,3,\ldots,k$, then $R(x)$ has a root α_1 in G.F.(p^n) which is impossible. Hence no root occurs with a greater multiplicity than shown. Since $\ell_1 + \ell_2 + \ldots + \ell_k \leq n$ the proof of

Lemma 1.1 is complete.

Theorem 1.3: A Galois field G.F.(p^n) of order p^n has $\phi(p^n-1)$ primitive roots where $\phi(n)$ denotes the number of residues modulo n which are prime to n.

Proof: Let s be the largest ~~integer~~ order occurring in G.F.(p^n). Since every order divides s we must have, for every $\alpha \neq 0$ in G.F.(p^n),

$$\alpha^s = 1. \tag{1.2}$$

Thus the polynomial in α, (1.2), has the roots $x_1,\ldots,x_{p^n-1}$; i.e., it has at least p^n-1 roots. But $p^n-1 = 0(s)$. Therefore $p^n-1 = s$. Thus there exists at least one primitive root. Let this primitive root be w. Then w^i, where $(i,p^n-1)=1$, is also a primitive root. For, let t be the order of w^i. Then $w^{it}=1$ and, since p^n-1 is the order of w then $it \equiv 0\ (p^n-1)$ or $t \equiv 0\ (p^n-1)$. But $w^{i(p^n-1)} = 1$ and we may conclude that $t = p^n-1$.

We shall now show that all the primitive roots may be obtained this way. Let v be any other primitive root and since w is also a primitive root, ~~where w^j, $j=1,2,\ldots,p^n-1$,~~ there exists an integer j such that $w^j = v$, $j < p^n-1$. Suppose that $(j,p^n-1) = k \neq 1$. Then $w^{j(p^n-1)/k} = w^{j/k[(p^n-1)]} = 1$ since $w^{j/k}$ is an element in G.F.(p^n). But $w^{j\left(\frac{p^n-1}{k}\right)}$ is equal to $v^{\frac{p^n-1}{k}}$ which is equal to 1 and thus v is not a primitive root. But this is a contradiction. Hence all primitive roots are of the form w^i, $(i,p^n-1)=1$, and the proof of Theorem 1.3 is complete.

Once a primitive root is known, the construction of a set of orthogonal Latin squares can be simplified considerably.

Let w be a primitive root and $0,1,x_3,\ldots,x_n$ be the elements of a finite field of order n. Then

$$\overline{L}_i = \begin{matrix} 0 & 1 & \ldots & x_n \\ w^{0+i} & 1+w^{0+i} & \ldots & x_n+w^{0+i} \\ w^{1+i} & 1+w^{1+i} & \ldots & x_n+w^{1+i} \\ \vdots & \vdots & & \vdots \\ w^{n-2+i} & 1+w^{n-2+i} & \ldots & x_n+w^{n-2+i} \end{matrix} \qquad (i=0,1,2,\ldots,n-2)$$

are n-1 orthogonal Latin squares, for, the elements in the first column are all the elements of G.F.(n^n) and thus we have an addition table as in (1.1) It should be observed that $\overline{L}_{i+1}$ is obtained from $\overline{L}_i$ by cyclically permuting the last n-1 rows.

We shall next construct a G.F.(p^m) for every m and every p. If m = 1 then the residues modulo p form a G.F.(p).

Consider the polynomials

$$p(x) = x^n + a_1x^{n-1} + \ldots + a_n$$

whose coefficients $a_1,\ldots, a_n$ are elements of a field.

Theorem 1.4: If p(x) and q(x) are polynomials with coefficients in a field F then there exists a polynomial d(x) such that

$$p(x) \equiv 0(d(x)) \ , \ q(x) \equiv 0(d(x))$$

and such that $p(x) \equiv 0(h(x))$ implies $d(x) \equiv 0(h(x))$. Also there exist polynomials a(x) and b(x) such that

$$a(x)p(x) + b(x)q(x) = d(x).$$

If d(x) has the first coefficient one then d(x) is called the greatest common divisor of p(x) and q(x) and we shall write

$$(p(x),q(x)) = d(x).$$

If d(x) satisfies the conditions of the above theorem then ad(x)

also satisfies these conditions for every non-zero element a of F. Thus if b is the first coefficient of d(x) then $b^{-1}d(x)$ also satisfies the conditions of the above theorem and the first coefficient will be 1. It follows that the greatest common divisor is uniquely determined.

Proof of Theorem 1.4: From the set of all possible expressions, d(x), of the form

$$a(x)p(x) + b(x)q(x) = d(x), \tag{1.3}$$

select a d(x) of the lowest possible degree where the polynomial zero is not considered to have a degree. We shall now show that the polynomial d(x) satisfies the conditions of the theorem. By long division there exists a polynomial h(x) such that

$$p(x) - h(x)d(x) = r(x) \tag{1.4}$$

where r(x) is either zero or has a degree less than that of d(x). Multiplying (1.4) by h(x) we have

$$h(x)a(x)p(x) + h(x)b(x)q(x) = p(x) - r(x).$$

Put $\bar{a}(x) = -\left[h(x)p(x) - 1\right]$, and $\bar{b}(x) = -\left[h(x)b(x)\right]$.

We then have

$$\bar{a}(x)p(x) + \bar{b}(x)q(x) = r(x).$$

Since d(x) has the lowest degree of all the polynomials of (1.3) it then follows that $r(x) = 0$. Thus $p(x) \equiv 0(d(x))$. By a similar argument $q(x) \equiv 0(d(x))$. Finally, if a polynomial h(x) is a factor of both p(x) and q(x), by (1.3) it is also a factor of d(x).

Definition: If a polynomial g(x) with coefficients in a field F has no divisor except $\bar{a}$ and $\bar{a}g(x)$ with $\bar{a}$ in F, then g(x) is called irreducible in F.

Congruences modulo a polynomial m(x) are now defined

in exactly the same way as congruences in the system of all integers. Then we calculate modulo m(x) by adding, subtracting, and multiplying in the same manner and by always replacing every polynomial f(x) by the residue of smallest degree obtained by dividing f(x) by m(x).

Theorem 1.5: If g(x) is irreducible in F then the residues modulo g(x) in the system $\mathcal{J}(x)$ of all polynomials with coefficients in F form a field.

Proof: We see that all the properties of a field hold except possibly the fact that an inverse exists. Thus we can show that Theorem 1.5 holds true if we can prove the following: To every $f(x) \not\equiv 0(g(x))$ there exists a q(x) such that $f(x)q(x) \equiv 1(g(x))$. In other words we must show that there exists a $\lambda(x)$ such that

$$f(x)q(x)-1 = \lambda(x)g(x).$$

Since g(x) is irreducible and $f(x) \not\equiv 0(g(x))$, we see that $(f(x), g(x)) = 1$. But by Theorem 1.4 we have shown that for any two polynomials f(x) and g(x) there exist two polynomials q(x) and $\lambda(x)$ such that a linear combination of the two given polynomials exists and is equal to the greastest common divisor (g.c.d.) of f(x) and g(x). Thus there exists a polynomial $-\lambda(x)$ such that

$$f(x)q(x)-\lambda(x)g(x)= 1.$$

Let F now be the finite field, G.F.(p) of residues modulo p. We then have

Corollary to Theorem 1.5: If g(x) of degree n with coefficients in G.F.(p) is irreducible in G.F.(p) then the

residues modulo g(x) form a Galois field with p^n elements.

Proof: Every polynomial with coefficients in G.F.(p) is, modulo g(x), congruent to one of the p^n polynomials

$$a_o + a_1 x + \ldots + a_{n-1} x^{n-1}$$

where $a_o, a_1, \ldots, a_{n-1}$ may be any one of the residues modulo p and there are p^n such polynomials.

Thus to construct a G.F.(p^n) we must find first an irreducible polynomial of degree n with coefficients in G.F.(p).

As an example the polynomial $x^2 + x + 1$ is irreducible modulo 2, for none of its roots are in the field modulo 2. Hence the residues $0, 1, x, x+1$ form a G.F.(2^2). Also

$$x^0 \equiv 1 (x^2 + x + 1),$$
$$x^1 \equiv x (x^2 + x + 1),$$
$$x^2 \equiv x + 1 (x^2 + x + 1).$$

Thus x is a primitive root of this Galois field. We now set up the addition table for the elements 0, 1, x, x+1.

	0	1	x	x+1
0	0	1	x	x+1
1	1	0	x+1	x
x	x	x+1	0	1
x+1	x+1	x	1	0

Since x is a primitive root, we obtain from the addition table three orthogonal Latin squares of side four by cyclically permuting the last three rows. Replace x by 2 and x+1

by 3. We obtain the following orthogonal Latin squares:

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

As a second illustration the polynomial x^2+x-1 is irreducible modulo 3 since $0^2+0-1\equiv 2(3)$, $1^2+1-1\equiv 1(3)$, $2^2+2-1\equiv 2(3)$. The element x is a primitive root for

$$x^0\equiv 1, \qquad x^4\equiv 2,$$
$$x^1\equiv x, \qquad x^5\equiv 2x,$$
$$x^2\equiv 2x+1, \qquad x^6\equiv x+2,$$
$$x^3\equiv 2x+2, \qquad x^7\equiv x+1.$$

Forming the addition table we have

0	0	1	2	x	x+1	x+2	2x	2x+1	2x+2
1	1	2	0	x+1	x+2	x	2x+1	2x+2	2x
2	2	0	1	x+2	x	x+1	2x+2	2x	2x+1
x	x	x+1	x+2	2x	2x+1	2x+2	0	1	2
x+1	x+1	x+2	x	2x+1	2x+2	2x	1	2	0
x+2	x+2	x	x+1	2x+2	2x	2x+1	2	0	1
2x	2x	2x+1	2x+2	0	1	2	x	x+1	x+2
2x+1	2x+1	2x+2	2x	1	2	0	x+1	x+2	x
2x+2	2x+2	2x	2x+1	2	0	1	x+2	x	x+1 .

Setting $x=3$ and cyclically permuting the last eight rows we obtain the following set of eight orthogonal Latin squares:

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

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

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

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

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

Lemma 1.2: Every modulo p irreducible polynomial of degree r is , mod p, a divisor of $x^{p^r-1}-1$.

The congruence relationship $a(x) \equiv b(x) \bmod (f(x),p)$ stated in full says that $a(x)-b(x)$ is divisible by $f(x)$ where the coefficients of $f(x)$ are elements of the G.F.(p). The set of polynomial residues mod $(f(x),p)$ form a Galois field of order p^r. Hence, since x is an element of the G.F.(p^r),

$$x^{p^r-1} \equiv 1 \ (f(x),p).$$

Therefore it follows that

$$x^{p^r-1}-1 \equiv 0 \ (f(x),p)$$

which is Lemma 1.2.

Lemma 1.3: If $f(x)$ is irreducible mod p and of degree $s > r$ then $f(x)$ is, mod p, not a divisor of $x^{p^r-1}-1$.

Assume that $x^{p^r-1}-1 \equiv 0 \ (f(x),p)$ and consider the Galois

field of residues mod $(f(x),p)$. The order of this Galois field is p^s. Every element of this Galois field is of the form $a_o+a_1x + \ldots + a_kx^k$, $k < s$, where the coefficients $a_o,a_1,..,a_k$ are residues mod p. By our assumption $x^{p^r} \equiv x(f(x),p)$. Now $(a_o + a_1x + \ldots + a_kx^k)^p = \sum_{q_0+q_1+\cdots q_k=p} \frac{p!}{q_0!q_1!\cdots q_k!} a_o^{q_0}a_1^{q_1} \ldots a_k^{q_k}x^{q_1+2q_2+\ldots+kq_k}$. Since the coefficients of a multinomial are integers, the $q_i!$, $i=0,1,2,\ldots,k$, are all factors of $p!$. Thus the coefficients are all multiples of p, since p is a prime, and hence congruent to zero mod p, exept in the case where one of the $q_i = p$ (causing the rest of the q_i's to be zero) in which case the factorial expression reduces to the value one. Thus we have

$$(a_o + a_1x + \ldots + a_kx^k)^p \equiv a_o^p + a_1^px^p + \ldots + a_k^px^{kp} \ (p).$$

By mathematical induction it may be shown that

$$(a_o + a_1x + \ldots + a_kx^k)^{p^r} \equiv a_o^{p^r} + a_1^{p^r}x^{p^r} + \ldots + a_k^{p^r}x^{kp^r} \ (p).$$

Since $a_i^{p^r} \equiv a_i \ (p)$[1], $i = 0,1,2,\ldots,k$, and also $x^{mp^r} \equiv x^m(f(x),p)$ for $m = 1,2,\ldots,k$, then it follows that

$$(a_o + a_1x + \ldots + a_kx^k)^{p^r} \equiv a_o + a_1x + \ldots + a_kx^k \ (f(x),p).$$

Hence the order of our G.F.(p^s) is p^s. Since $s > r$, this is impossible. Thus we conclude that $x^{p^r-1}-1 \not\equiv 0 \ (f(x),p)$.

Definition: The derivative with respect to x of a polynomial

$$f(x) \equiv a_o + a_1x + a_2x^2 + \ldots + a_nx^n \ (p)$$

is

$$f'(x) \equiv a_1 + 2a_2x + \ldots + na_nx^{n-1} \ (p).$$

---

[1] MacDuffee,C.C. Introduction to Abstract Algebra. New York: Wiley, 1940, p. 25.

Theorem 1.6: The derivative of an integer is congruent to zero. The derivative of x is congruent to one. The derivative of a sum is congruent to the sum of the derivatives. The derivative of a product $f(x)g(x)$ is congruent to

$$f'(x)g(x)+f(x)g'(x) \quad (p).$$

The proofs of the first three statements follow directly from the definition above. To prove the fourth statement, set

$$f(x)\equiv\sum_{i=0}^{\ell}a_i x^i\ , \quad g(x)\equiv\sum_{j=0}^{n}b_j x^j\ ,$$

$$f(x)g(x)\equiv\sum_{i=0}^{\ell}\sum_{j=0}^{n}a_i b_j x^{i+j} \quad (p).$$

Thus the derivative of $f(x)g(x)$ is then

$$\sum_{i=0}^{\ell}\sum_{j=0}^{n}(i+j)a_i b_j x^{i+j-1}\equiv\sum_{i=0}^{\ell}ia_i x^{i-1}\sum_{j=0}^{n}b_j x^j+\sum_{i=0}^{\ell}a_i x^i\sum_{j=0}^{n}jb_j x^{j-1}$$
$$\equiv f'(x)g(x)+f(x)g'(x) \quad (p).$$

Theorem 1.7: If $(x-x_1)^h$ is the highest power of $x-x_1$ which divides $f(x)$, and if $(p,h)=1$, then $(x-x_1)^{h-1}$ is the highest power of $x-x_1$ which divides $f'(x)$.

Proof: Let $f(x)\equiv(x-x_1)^h g(x)$. Then by the above theorem

$$f'(x)\equiv(x-x_1)^h g'(x)+h(x-x_1)^{h-1}g(x)$$
$$\equiv(x-x_1)^{h-1}\left[(x-x_1)g'(x)+hg(x)\right]\ ,$$

and thus $(x-x_1)^{h-1}$ divides $f'(x)$, mod p. Now if $(x-x_1)^h$ is the highest power of $x-x_1$ that divides $f(x)$, $x-x_1$ cannot divide $g(x)$, and since $(p, h)=1$, $x-x_1$ cannot divide $\left[(x-x_1)g'(x)+hg(x)\right]$ since $hg(x)\not\equiv 0$, mod p. Thus $(x-x_1)^{h-1}$ is the highest power of $x-x_1$ which divides $f'(x)$, mod p.

Lemma 1.4: The polynomial x^m-1 has no double roots mod p if $m\not\equiv 0$ (p).

We see that, from Theorem 1.7, if $f(x)$ has a double root then $f(x)$ and df/dx have a common factor by putting $h=2$. If x^m-1 and mx^{m-1} have, mod p, a common root, sav α, then

$$\alpha^m-1\equiv 0\ (p)\ ,\quad m\alpha^{m-1}\equiv 0\ (p).$$

Since $(m,p)=1$,

$$\alpha^m\equiv 1\ (p)\ \text{and}\ \alpha^m\equiv 0\ (p)$$

which is impossible.

Theorem 1.8: There exists a Galois field of order p^r for everv prime p and every r.

Proof: The polynomial $x^{p^r-1}-1$ contains, mod p, no irreducible factor of degree $>r$, by lemma 1.3. All the irreducible polynomials of degree $f<r$ are, mod p, factors of $x^{p^r-1}-1$, by lemma 1.2. Now consider all the irreducible factors of $x^{p^r-1}-1$ of degree $f<r$. By lemma 1,2 these factors, if any, are all in $x^{p^f-1}-1$ and by lemma 1.4 they occur at most once in $x^{p^f-1}-1$. Hence the sum of the degrees of these factors cannot exceed the degree of $x^{p^f-1}-1$. Thus the sum of the degrees of all the factors of degree less than r is at most

$$\sum_{\beta=1}^{\lambda-1}(p^f-1)<\sum_{\beta=1}^{\lambda-1}p^f=\frac{p^f-p}{p-1}<\frac{p^r-1}{p-1}\leqslant p^r-1.$$

The factors, if any, that are of degree $<r$, which are reducible are included in the irreducible factors of degree $<r$. Thus there is at least one irreducible factor of degree r. Let $f(x)$ be this polynomial. Then the polynomial set of residues of the form

$$a_o+a_1x+\ldots+a_{r-1}x^{r-1}\ (f(x),p)$$

form a Galois field of order p^r by the corollary to Theorem 1.5.

Definition: Two fields F and F' are called isomorphic if there exists a bi-unique correspondence $a \longleftrightarrow a'$, a in F, a' in F', such that $a \longleftrightarrow a'$, $b \longleftrightarrow b'$ implies $a+b \longleftrightarrow a'+b'$, $ab \longleftrightarrow a'b'$.

Theorem 1.7: Any two Galois fields with p^n marks are isomorphic.[1]

We have thus essentially only one Galois field with p^n marks. We shall refer to this field as G.F.(p^n). Let α be any primitive root of the Galois field. This root satisfies the equation

$$x^{p^n-1}-1=0.$$

Consider the elements of the form $a_0+a_1x+\ \ldots+a_{n-1}x^{n-1}$. Among these elements are the elements of our set of residues, mod p, which we call the integral marks of the G.F.(p^n). Hence α satisfies a polynomial equation whose coefficients are integral marks of the field. Let k be the lowest degree of such equations satisfied by α. Then α satisfies an equation of the form

$$\gamma_k x^k+\gamma_{k-1}x^{k-1}+\ldots+\gamma_1 x+\gamma_0=0 \tag{1.5}$$

where $\gamma_k \neq 0$. If k is to be the lowest degree for such an equation satisfied by α, then (1.5) is an irreducible equation in the sense that the first member cannot be separated into factors of positive ~~integers~~ degree with coefficients which are integral marks of the field since otherwise k would not be the lowest degree. Thus α^k and hence every power of α can be expressed in the

---

[1] Birkoff G. and McLane S, A Survey of Modern Algebra. New York: MacMillan, 1948, p. 429.

form

(1.6) $$\gamma_{k-1}\alpha^{k-1} + \gamma_{k-2}\alpha^{k-2} + \cdots + \gamma_1\alpha + \gamma_0$$

where $\gamma_0, \gamma_1, \ldots, \gamma_{k-1}$ are integral marks of the field not all zero. Suppose that α^m can be expressed by the following two expressions, viz.,

(1.7) $$\alpha^m = \beta_{k-1}\alpha^{k-1} + \beta_{k-2}\alpha^{k-2} + \cdots + \beta_0 ,$$

$$\alpha^m = \delta_{k-1}\alpha^{k-1} + \delta_{k-2}\alpha^{k-2} + \cdots + \delta_0 ,$$

from which we obtain

$$(\delta_{k-1} - \beta_{k-1})\alpha^{k-1} + (\delta_{k-2} - \beta_{k-2})\alpha^{k-2} + \ldots + \delta_0 - \beta_0 = 0.$$

But this equation satisfied by α is of degree k-1 which is less than k. This is impossible. Therefore α^m has a unique representation in the form (1.7). But every non-zero element of this field is given by α^m for some value of m. Thus every non-zero element of the field is given by

$$\gamma_{k-1}\alpha^{k-1} + \gamma_{k-2}\alpha^{k-2} + \cdots + \gamma_0$$

in one and only one way. The number of ways of writing (1.7) is p^k-1 (the -1 for the case where $\gamma_0 = \gamma_1 = \cdots = \gamma_{k-1} = 0$). But every expression of this form is an element of the field. Hence the p^k-1 possible non-zero forms are all the p^n-1 non-zero elements of the field. Therefore

$$p^n - 1 = p^k - 1$$

from which it follows that $n = k$. Hence

Theorem 1.10: A primitive root of a G.F.(p^n) satifies an irreducible equation of the form

$$x^n + c_1x^{n-1} + \ldots + c_n = 0$$

where $c_1, c_2, \ldots, c_n$ are integral marks of the G.F.(p^n).

Corollary 1: A primitive root satisfies no equation of degree less than n, the coefficients of which are integral marks of the G.F.(p^n).

Proof: In the proof of the above theorem we saw that the lowest degree was n.

Corollary 2: The quotient

$$\frac{x^{p^n}-x}{x^n+c_1x^{n-1}+\cdots+c_n}$$

can be expressed as a polynomial in x with coefficients which are integral marks of the field.

Proof: This is equivalent to Lemma 1.2.

For any x in the field of residues mod (f(x),p) if $x^m-1\not\equiv 0$ (f(x),p) for $m<p^n-1$ and $x^m-1\equiv 0$ (f(x),p) for $m=p^n-1$ then x is a primitive root. Then if G.F.(p^n) is to be represented by the residues mod (f(x),p) in such a way that x is to be a primitive root we must remove from $x^{p^n-1}-1$ all the factors which are also factors of x^m-1 for $m<p^n-1$. Hence the remaining polynomial has as its roots all the primitive roots of G.F.(p^n) and by Theorem 1.3 it has degree $\phi(p^n-1)$. This is called the cyclotomic polynomial of order p^n-1.

As an example, to construct G.F.(2^3) form the cyclotomic polynomial of order $2^3-1=7$. Its degree is $\phi(7)=6$. Since x-1 is a factor of x^7-1 where $m=1<7$, dividing out the factor x-1 from x^7-1 we obtain

$$x^6+x^5+x^4+x^3+x^2+x+1.$$

By Theorem 1.10, this polynomial must, mod 2, decompose into two

factors of degree three each. Thus

$(x^6+x^5+x^4+x^3+x^2+x+1) \equiv (x^3+ax^2+bx+c)(x^3+\bar{a}x^2+\bar{b}x+c)$ (2).

Hence, equating the constant terms, we have $c\bar{c} \equiv 1$ (2) and $c=\bar{c}=1$. The coefficient of x is $c\bar{b}+\bar{c}b=b+\bar{b} \equiv 1$ (2). We may take $b=0$, $\bar{b}=1$. The coefficient of x^2 is $a\bar{c}+\bar{a}c+b\bar{b}=a+\bar{a} \equiv 1$ (2). The coefficient of x^3 is $c+\bar{c}+a\bar{b}+\bar{a}b \equiv a \equiv 1$ (2). Hence $a=1$ and $\bar{a}=0$. Therefore

$$x^6+x^5+x^4+x^3+x^2+x+1 \equiv (x^3+x^2+1)(x^3+x+1) \quad (2).$$

Since x^3+x+1 is irreducible mod 2, then

$x^0 \equiv 1$, $x^4 \equiv x^2+x$,

$x^1 \equiv x$, $x^5 \equiv x^2+x+1$,

$x^2 \equiv x^2$, $x^6 \equiv x^2+1$,

$x^3 \equiv x+1$, $x^7 \equiv 1$,

from which we see that x is a primitive root. Forming the addition table we have

	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	x+1	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	x+1	0	1	x^2+x	x^2+x+1	x^2	x^2+1
x+1	x+1	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	x+1
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	x+1	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	x+1	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	x+1	x	1	0.

Setting $x=2$ and cyclically permuting the last seven rows we

obtain the following set of seven orthogonal Latin squares of side eight:

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

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

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

0 1 2 3 4 5 6 7

7 6 5 4 3 2 1 0

1 0 3 2 5 4 7 6

2 3 0 1 6 7 4 5

3 2 1 0 7 6 5 4

4 5 6 7 0 1 2 3

5 4 7 6 1 0 3 2

6 7 4 5 2 3 0 1 .

If we use the method of decomposing the cyclotomic polynomial of order p^r-1, it becomes rather laborious to find mod p irreducible polynomials of degree r for higher values of p^r-1. Should we be willing to dispense with the advantage of having x as a primitive root then we can find irreducible polynomials by other methods. For instance, if p is odd then there always exist# residues a for which $x^2 \equiv a\ (p)$ has no solution.[1] Hence x^2-a is irreducible mod p. The polynomial $x^3+2x \equiv 0\ (3)$ for $0+0 \equiv 0\ (3)$, $1^3+2 \equiv 0\ (3)$, and $2^3+2^2 \equiv 0\ (3)$. Hence $x^3+2x+1 \not\equiv 0\ (3)$. This shows that x^3+2x+1 has no linear factors, mod 3, and hence the expression x^3+2x+1 is irreducible mod 3. The polynomial x^4+x+1 is irreducible mod 2. Since 0 and 1 are not roots, there cannot be any linear factors of x^4+x+1. Hence the only possible decomposition would be of the form

$$x^4+x+1 \equiv (x^2+bx+1)(x^2+\bar{b}x+1)\ (2).$$

---

[1] Uspensky and Heaslet, Elementary Number Theory. pp. 203-204.

Equating coefficients we get the following congruence relationships: $b+\bar{b} \equiv 1 \ (2)$ and $b+\bar{b} \equiv 0 \ (2)$ which is impossible. In a similar manner we can obtain the following irreducible polynomials:

mod 2: x^2+x+1, x^3+x+1, x^4+x+1, x^5+x^2+1;

mod 3: x^2+x+2, x^3+2x+1;

mod 5: x^2+2;

mod 7: x^2+1.

This set accounts for all the Galois fields with less than 63 elements and these satisfy all the needs that have arisen to date in the design of experiments.

From Theorem 1.8 and Theorem 1.1 we see that a set of m-1 orthogonal Latin squares of side m can always be constructed if m is the power of a prime. If m is not the power of a prime then m can be decomposed into prime powers such that

$$m = p_1^{e_1} \cdots p_s^{e_s} \text{ where } p_i \neq p_j \text{ for } i,j = 1,2,\ldots,s.$$

Next construct the following system in which we consider the "points"

$$\gamma = (g^{(1)}, g^{(2)}, \ldots, g^{(s)}), \quad g^{(i)} \text{ in G.F.}(p_i^{(e_i)}).$$

Addition and multiplication are defined by the rules

$$\gamma_1 \overset{+}{x} \gamma_2 = (g_1^{(1)}, g_1^{(2)}, \ldots, g_1^{(s)}) \overset{+}{x} (g_2^{(1)}, g_2^{(2)}, \ldots, g_2^{(s)})$$

$$= (g_1^{(1)} \overset{+}{x} g_2^{(1)}, g_1^{(2)} \overset{+}{x} g_2^{(2)}, \ldots, g_1^{(s)} \overset{+}{x} g_2^{(s)}).$$

As an illustration, consider $m = 12$. We decompose 12 into its prime powers, viz.,

$$12 = 2^2 \cdot 3^1.$$

We have already found that the elements of the G.F.(2^2) are

$0,1,x$, and $x+1$. The G.F.(3) consists of the marks 0,1,2. From these two fields construct the following set of "points": $(0,0)$, $(0,1)$, $(0,x)$, $(0,x+1)$, $(1,0)$, $(1,1)$, $(1,x)$, $(1,x+1)$, $(2,0)$, $(2,1)$, $(2,x)$, $(2,x+1)$. The addition of two "points", say $(1,x)$ and $(2,x+1)$, by definition, gives

$$(1,x)+(2,x+1)=(0,1)$$

since $1+2\equiv 0$ (3) and $x+x+1\equiv 1$ $(x^2+x+1,2)$. Also the multiplication of these "points" gives, by definition,

$$(1,x)\times(2,x+1)=(2,1)$$

since $(1)(2)\equiv 2$ (3) and $(x)(x+1)\equiv 1$ $(x^2+x+1,2)$.

The system constructed is not a field, since the element $(0,1,1,\ldots,1)$ has no multiplicative inverse. However, referring to the postulates governing a field, we see that conditions I-IV for addition and I-III for multiplication and postulate V are fulfilled. All the "points" which have no zero among their coordinates possess inverses. In general the identity element for addition is $(0,0,\ldots,0)$ and that for multiplication is $(1,1,\ldots,1)$.

Let

$$0,\ g_1^{(i)}=1,\ g_2^{(i)},\ldots,\ g_{p_i^{e_i}-1}^{(i)},$$

be the marks of G.F.$(p_i^{e_i})$. Then, if $r=\min_i(p_i^{e_i}-1)$, the "points"

$$\gamma_j=(g_j^{(1)},\ g_j^{(2)},\ldots,g_j^{(s)}) \qquad 0<j\leq r \tag{1.8}$$

possess inverses and also $\gamma_j-\gamma_i$ has an inverse if $j\neq i$ since γ_i and γ_j contain no zero among their coordinates and corresponding coordinates are different elements from the same field. We now number the "points" γ in such a way that the first r marks are given by (1.8) and construct the arrays L_j which form the body

of the addition tables:

	0	1	$\cdots$	γ_{m-1}	
0	0	1	$\cdots$	γ_{m-1}	
(1.9) γ_j	γ_j	γ_j+1	$\cdots$	$\gamma_j+\gamma_{m-1}$	$(j = 1,2,\ldots,r)$
$\gamma_j\gamma_2$	$\gamma_j\ \gamma_2$	$\gamma_j\ \gamma_2+1$	$\cdots$	$\gamma_j\ \gamma_2+\gamma_{m-1}$	
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
$\gamma_j\gamma_{m-1}$	$\gamma_j\ \gamma_{m-1}$	$\gamma_j\ \gamma_{m-1}+1$	$\cdots$	$\gamma_j\gamma_{m-1}+\gamma_{m-1}$	.

Continuing with our example we have that $p_1^{e_1} = 2^2$ and $p_2^{e_2} = 3^1$ from which $r = \min_i(p_i^{e_i}-1) = 2$. Therefore we will have two arrays of the form (1.9). First, we find γ_1 and γ_2. By definition $\gamma_1 = (g_1^{(1)}, g_1^{(2)}) = (1,1)$ and $\gamma_2 = (g_2^{(1)}, g_2^{(2)}) = (2,x)$. Next form table L_1 by putting $j = 1$ in (1.9). Thus we have L_1 given by the table on the following page. In order to get the second table, L_2, set $j = 2$ and proceed as in (1.9). This gives us the table L_2 on page 32.

$L_1 =$

	(0,0)	(1,1)	(2,x)	(0,1)	(0,x)	(0,x+1)	(1,0)	(1,x)	(1,x+1)	(2,0)	(2,1)	(2,x+1)
(0,0)	(0,0)	(1,1)	(2,x)	(0,1)	(0,x)	(0,x+1)	(1,0)	(1,x)	(1,x+1)	(2,0)	(2,1)	(2,x+1)
(1,1)	(1,1)	(2,0)	(0,x+1)	(1,0)	(1,x+1)	(1,x)	(2,1)	(2,x+1)	(2,x)	(0,1)	(0,0)	(0,x)
(2,x)	(2,x)	(0,x+1)	(1,0)	(2,x+1)	(2,0)	(2,1)	(0,x)	(0,0)	(0,1)	(1,x)	(1,x+1)	(1,1)
(0,1)	(0,1)	(1,0)	(2,x+1)	(0,0)	(0,x+1)	(0,x)	(1,1)	(1,x+1)	(1,x)	(2,1)	(2,0)	(2,x)
(0,x)	(0,x)	(1,x+1)	(2,0)	(0,x+1)	(0,0)	(0,1)	(1,x)	(1,0)	(1,1)	(2,x)	(2,x+1)	(2,1)
(0,x+1)	(0,x+1)	(1,x)	(2,1)	(0,x)	(0,1)	(0,0)	(1,x+1)	(1,1)	(1,0)	(2,x+1)	(2,x)	(2,0)
(1,0)	(1,0)	(2,1)	(0,x)	(1,1)	(1,x)	(1,x+1)	(2,0)	(2,x)	(2,x+1)	(0,0)	(0,1)	(0,x+1)
(1,x)	(1,x)	(2,x+1)	(0,0)	(1,x+1)	(1,0)	(1,1)	(2,x)	(2,0)	(2,1)	(0,x)	(0,x+1)	(0,1)
(1,x+1)	(1,x+1)	(2,x)	(0,1)	(1,x)	(1,1)	(1,0)	(2,x+1)	(2,1)	(2,0)	(0,x+1)	(0,x)	(0,0)
(2,0)	(2,0)	(0,1)	(1,x)	(2,1)	(2,x)	(2,x+1)	(0,0)	(0,x)	(0,x+1)	(1,0)	(1,1)	(1,x+1)
(2,1)	(2,1)	(0,0)	(1,x+1)	(2,0)	(2,x+1)	(2,x)	(0,1)	(0,x+1)	(0,x)	(1,1)	(1,0)	(1,x)
(2,x+1)	(2,x+1)	(0,x)	(1;1)	(2,x)	(2,1)	(2,0)	(0,x+1)	(0,1)	(0,0)	(1,x+1)	(1,x)	(1,0)

$L_2 =$

	(0,0)	(1,1)	(2,x)	(0,1)	(0,x)	(0,x+1)	(1,0)	(1,x)	(1,x+1)	(2,0)	(2,1)	(2,x+1)
(0,0)	(0,0)	(1,1)	(2,x)	(0,1)	(0,x)	(0,x+1)	(1,0)	(1,x)	(1,x+1)	(2,0)	(2,1)	(2,x+1)
(2,x)	(2,x)	(0,x+1)	(1,0)	(2,x+1)	(2,0)	(2,1)	(0,x)	(0,0)	(0,1)	(1,x)	(1,x+1)	(1,1)
(1,x+1)	(1,x+1)	(2,x)	(0,1)	(1,x)	(1,1)	(1,0)	(2,x+1)	(2,1)	(2,0)	(0,x+1)	(0,x)	(0,0)
(0,x)	(0,x)	(1,x+1)	(2,0)	(0,x+1)	(0,0)	(0,1)	(1,x)	(1,0)	(1,1)	(2,x)	(2,x+1)	(2,1)
(0,x+1)	(0,x+1)	(1,x)	(2,1)	(0,x)	(0,1)	(0,0)	(1,x+1)	(1,1)	(1,0)	(2,x+1)	(2,x)	(2,0)
(0,1)	(0,1)	(1,0)	(2,x+1)	(0,0)	(0,x+1)	(0,x)	(1,1)	(1,x+1)	(1,x)	(2,1)	(2,0)	(2,x)
(2,0)	(2,0)	(0,1)	(1,x)	(2,1)	(2,x)	(2,x+1)	(0,0)	(0,x)	(0,x+1)	(1,0)	(1,1)	(1,x+1)
(2,x+1)	(2,x+1)	(0,x)	(1,1)	(2,x)	(2,1)	(2,0)	(0,x+1)	(0,1)	(0,0)	(1,x+1)	(1,x)	(1,0)
(2,1)	(2,1)	(0,0)	(1,x+1)	(2,0)	(2,x+1)	(2,x)	(0,1)	(0,x+1)	(0,x)	(1,1)	(1,0)	(1,x)
(1,0)	(1,0)	(2,1)	(0,x)	(1,1)	(1,x)	(1,x+1)	(2,0)	(2,x)	(2,x+1)	(0,0)	(0,1)	(0,x+1)
(1,x)	(1,x)	(2,x+1)	(0,0)	(1,x+1)	(1,0)	(1,1)	(2,x)	(2,0)	(2,1)	(0,x)	(0,x+1)	(0,1)
(1,1)	(1,1)	(2,0)	(0,x+1)	(1,0)	(1,x+1)	(1,x)	(2,1)	(2,x+1)	(2,x)	(0,1)	(0,0)	(0,x)

In order to simplify the tables, L_1 and L_2, assign the numbers 0,1,2,...,11 to the set of "points" (0,0),(1,1),(2,x), (0,1),.. ., (2,x+1) respectively; i.e., set (0,0) = 0, $\gamma_1 = 1$, $\gamma_2 = 2, \ldots, \gamma_{11} = 11$. Considering the inner squares only, we have

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

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

as our representations of L_1 and L_2.

We prove first that (1.9) is a Latin square. Suppose the αth row could contain an element twice, say in the k+1 th and ℓ+1 th columns. Then

$$\gamma_j \gamma_{\alpha-1} + \gamma_k = \gamma_j \gamma_{\alpha-1} + \gamma_\ell .$$

Since $\gamma_j \gamma_{\alpha-1}$ has an additive inverse, we obtain $\gamma_k = \gamma_\ell$, from which it follows that $k = \ell$. Suppose that the ith column contains the same element twice. Then

$$\gamma_{i-1} + \gamma_j \gamma_\alpha = \gamma_{i-1} + \gamma_\delta \gamma_\beta \qquad \text{where } j \leq r.$$

Since γ_j has a multiplicative inverse, this implies that $\gamma_\alpha = \gamma_\beta$, from which $\alpha = \beta$. From the argument presented we have shown that no element occurs more than once in each row and in each column. Since the set of "points" is closed under addition and multiplication, every element must occur once in every row and every column. Hence (1.9) is a Latin square.

We shall now prove that L_i is orthogonal to L_j, if $i \neq j$. Suppose that they are not orthogonal. Superimposing L_i on L_j, we should have two cells in the resulting square containing the same ordered pair of "points". If this pair occurs in the αth row and βth column in one and in the σth row and τth column in the other, we should have

$$\gamma_j \gamma_{\alpha-1} + \gamma_{\beta-1} = \gamma_j \gamma_{\sigma-1} + \gamma_{\tau-1},$$

$$\gamma_i \gamma_{\alpha-1} + \gamma_{\beta-1} = \gamma_i \gamma_{\sigma-1} + \gamma_{\tau-1}.$$

Subtracting, we have

$$(\gamma_i - \gamma_j)\gamma_{\alpha-1} = (\gamma_i - \gamma_j)\gamma_{\sigma-1}.$$

Since $\gamma_i - \gamma_j$ has an inverse for $i \neq j$, it follows that $\gamma_{\alpha-1} = \gamma_{\sigma-1}$, which implies that $\alpha = \sigma$. This in turn implies that $\beta = \tau$. As a result we have

Theorem 1.11: Let $g_{i_1}^{(1)}, g_{i_2}^{(2)}, \ldots, g_{i_s}^{(s)}$, denote the elements of the G.F.$(p_1^{e_1}), \ldots,$G.F.$(p_s^{e_s})$ respectively, where $g_o^{(i)}$ is the zero element and $g_1^{(i)}$ is the unity element of G.F.$(p_i^{e_i})$. From the "points"

$$\gamma = (g_{i_1}^{(1)}, g_{i_2}^{(2)}, \ldots, g_{i_s}^{(s)})$$

which are multiplied and added by multiplying and adding their coordinates. Further, let

$$\gamma_j = (g_j^{(1)}, g_j^{(2)}, \ldots, g_j^{(s)}), \quad 0 < j \leq r = \min_i (p_i^{e_i} - 1)$$

and number the remaining "points" in any arbitrary way from $r+1$ to $m = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$ in such a way that $\gamma_m = 0 = (g_o^{(1)}, g_o^{(2)}, \ldots, g_o^{(s)})$. Then the arrays

$$L_j = \begin{matrix} 0 & 1 & \cdots & \gamma_{m-1} \\ \gamma_j & \gamma_j+1 & \cdots & \gamma_j+\gamma_{m-1} \\ \gamma_j\gamma_2 & \gamma_j\gamma_2+1 & \cdots & \gamma_j\gamma_2+\gamma_{m-1} \\ \vdots & \vdots & & \vdots \\ \gamma_j\gamma_{m-1} & \gamma_j\gamma_{m-1}+1 & \cdots & \gamma_j\gamma_{m-1}+\gamma_{m-1} \end{matrix} \qquad (j = 1,2,\ldots,r)$$

form a set of orthogonal Latin squares.

This result is the best that has been obtained up to date. No case of more than $r = \min_i(p_i^{e_i}-1)$ orthogonal squares is known up to the present time. Tarry (Le Probleme de 36 Officiers. Comptes Rendus de l'Association Francaise pour L'avancement des Sciences II (1901) pp. 170-203) found by a skillful, tactical enumeration that no six-sided orthogonal pair exists. R.H.Bruck and H.J.Ryser have since proved (Canad. J. of Math. Vol. 1, pp. 88-93) the non-existence of m-1 orthogonal squares of side m if $m = 1,2,(4)$ and the square free part of m is divisible by a prime of the form $4k+3$. For numbers greater than six which are not powers of a prime the problem has remained unsolved although this problem has been confronting mathematicians long before Latin squares were applied in the design of experiments.

It can be shown that not more than m-1 orthogonal Latin squares of side m can exist. For let r be the maximum number

of orthogonal Latin squares of side m. By renumbering we can make the elements of the first row of each of these renumbered Latin squares be 1,2,...,m. Each of these renumbered Latin squares is still a Latin square. If we take any two of the renumbered squares we still get the m^2 different pairs as before but in a different order and hence the two squares are still orthogonal. For any two squares the ordered number pairs in the first row are (1,1),(2,2),...,(m,m). The ordered pair in the second row and first column must consist of numbers not equal to each other since all pairs of equal numbers appear in the first row. Hence the numbers appearing in the second row and first column of our r orthogonal Latin squares must be different from each other and selected from the m-1 numbers 2,3,..., m. Hence the maximum number of orthogonal Latin squares of side m cannot exceed m-1.

Historically it may be remarked that the proof of the existence of m-1 orthogonal Latin squares if m is a prime power seems to have been given by McNeish (Annals of Mathematics, Vol. XIII, pp. 221-227.) The methods for the construction of orthogonal Latin squares presented in this chapter are due to R.C.Bose. (Sankhya 1939).

CHAPTER II

THE CONSTRUCTION OF INCOMPLETE BALANCED BLOCK DESIGNS

An incomplete balanced block design is any arrangement of v varieties into b blocks of k plots each, such that:

(1) no block contains the same variety twice;

(2) every variety is repeated r times;

(3) every variety v_i occurs with every other variety v_j in exactly λ blocks.

Finite projective geometries are used extensively in the construction of incomplete balanced block designs and produce whole series of these designs. It will be sufficient for the work presented here that we consider finite analytic geometries. Several of the main concepts will now be defined. We shall consider the G.F.(p^n). A point in the m dimensional finite geometry P.G.(m,p^n) is an ordered set of $m+1$ elements of the G.F.(p^n), not all of which are equal to zero. Two sets $(g_1,g_2,\ldots,g_{m+1})$, $(g_1',g_2',\ldots,g_{m+1}')$ represent the same point if $g_i = \lambda g_i'$, $i = 0,1,2,\ldots,m+1$, for some $\lambda \neq 0$ and in the G.F.(p^n). For any two distinct points $p_1 = (g_1,g_2,\ldots,g_{m+1})$, $p_2 = (g_1', g_2', \ldots,g_{m+1}')$, we define as the line joining them the set of all points of the form

$$\lambda_1 p_1 + \lambda_2 p_2 = (\lambda_1 g_1 + \lambda_2 g_2', \ldots, \lambda_1 g_{m+1} + \lambda_2 g_{m+1}'),$$

where λ_1, λ_2, are in the G.F.(p^n), and where at least one of the λ's is different from zero.

This set of lines and points is called the analytic

projective geometry of the G.F.(p^n) of m dimensions and is denoted by P.G.(m,p^n).

As an example consider the G.F.(2^2) whose elements are $0,1,x,x+1$. The point $(0,1,x,x)$ in the P.G.($3,2^2$) is the same as the point $(0,x+1,1,1)$ since the second point may be obtained by multiplying the first point by $\lambda=x+1$.

First, we find the total number of points in a P.G.(m,p^n). Taking all possible selections of m+1 elements of the P.G.(m,p^n) there are $p^{n(m+1)}$ ordered sets. Since, from above, the set $(0,0,\ldots,0)$ must be excluded, the total number of ordered sets that have at least one non-zero element is $p^{n(m+1)}-1$. Since $(g_1,g_2,\ldots,g_{m+1}) = (\lambda g_1, \lambda g_2,\ldots, \lambda g_{m+1})$ for all $\lambda \neq 0$ in the G.F.(p^n), the ordered sets above may be divided into groups of p^n-1 sets, the members of a given group represent the same point. Thus the number of distinct points is

$$\frac{p^{n(m+1)}-1}{p^n-1} = 1+p^n+\ldots+p^{nm}.$$

The lines are given by the form $\lambda_1 p_1 + \lambda_2 p_2$ where p_1 and p_2 are distinct points. The points of this line are given by their line coordinates λ_1, λ_2. Two points $\lambda_1, \lambda_2, \mu_1, \mu_2$, will be distinct if $(\lambda_1, \lambda_2) \neq \nu(\mu_1, \mu_2)$ for all ν in G.F.(p^n). Hence the points of a line form an analytic one dimensional geometry.

We have seen that the number of points in such a geometry is p^n+1. Thus the number of points on a line is p^n+1.

Consider next the k dimensional subspaces of the P.G.(m, p^n). Let $p_1,p_2,\ldots,p_{k+1}$ be k+1 linearly independent points.

This means that the relation

$$\lambda_1 p_1 + \cdots + \lambda_{k+1} p_{k+1} = (0,0,\ldots,0),$$

implies that $\lambda_1 = \lambda_2 = \cdots = \lambda_{k+1} = 0$. Consider next all points of the form $\lambda_1 p_1 + \lambda_2 p_2 + \cdots + \lambda_{k+1} p_{k+1}$. These, by definition, form a k dimensional subspace. Suppose that two of these points are equal. Then

$$\lambda_1 p_1 + \lambda_2 p_2 + \cdots + \lambda_{k+1} p_{k+1} = \nu(\mu_1 p_1 + \mu_2 p_2 + \cdots + \mu_{k+1} p_{k+1}),$$

$$(\lambda_1 - \nu\mu_1) p_1 + (\lambda_2 - \nu\mu_2) p_2 + \cdots + (\lambda_{k+1} - \nu\mu_{k+1}) p_{k+1} = (0,0,\ldots,0).$$

Since $p_1, p_2, \ldots, p_{k+1}$ are linearly independent points, this implies that

$$\lambda_1 = \nu\mu_1, \quad \lambda_2 = \nu\mu_2, \quad \ldots, \quad \lambda_{k+1} = \nu\mu_{k+1}.$$

Thus we may represent a point in the k dimensional subspace by coordinates $(\lambda_1, \lambda_2, \ldots, \lambda_{k+1})$. For $k \geq 1$, the subspaces contain, for every two points, the line joining them. For, consider the k dimensional space consisting of all the points

$$\lambda_1 p_1 + \lambda_2 p_2 + \cdots + \lambda_{k+1} p_{k+1}$$

where the λ_i's are not all zero. Represent any two points by

$$P_1 = \lambda_{11} p_1 + \lambda_{21} p_2 + \cdots + \lambda_{k+1,1} p_{k+1},$$

$$P_2 = \lambda_{12} p_1 + \lambda_{22} p_2 + \cdots + \lambda_{k+1,2} p_{k+1},$$

where

$$(\lambda_{11}, \lambda_{21}, \ldots, \lambda_{k+1,1}) \neq \nu(\lambda_{12}, \lambda_{22}, \ldots, \lambda_{k+1,2})$$

for all ν in the G.F.(p^n). The points of the line determined by P_1 and P_2 are given by

$$\mu_1 P_1 + \mu_2 P_2 = \mu_1 \sum_{i=1}^{k+1} \lambda_{i1} p_i + \mu_2 \sum_{i=1}^{k+1} \lambda_{i2} p_i$$

$$= \sum_{i=1}^{k+1} (\mu_1 \lambda_{i1} + \mu_2 \lambda_{i2}) P_i .$$

The points are in the k dimensional space if the coefficients of the P_i's are not all zero. We may assume $\mu_1 \neq 0, \mu_2 \neq 0$, since P_1 and P_2 are in the k dimensional space. If

$$\mu_1 \lambda_{i1} + \mu_2 \lambda_{i2} = 0 , \qquad i = 1,2,\ldots,k+1,$$

then

$$\lambda_{i1} = -\frac{\mu_2}{\mu_1} \lambda_{i2}$$

and hence $P_1 = P_2$, which is impossible. Hence the coefficients are not all zero and $\mu_1 P_1 + \mu_2 P_2$ lies in the k dimensional space. We conclude that every k dimensional subspace of a P.G.(m,p^n) is itself a P.G.(k,p^n) and therefore consists of $1 + p^n + \ldots + p^{kn}$ points.

Consider any two distinct points, say p_1 and p_2, of the P.G.(k,p^n). If p_1 and p_2 are linearly dependent there exist λ_1 and λ_2 not both zero such that $\lambda_1 p_1 + \lambda_2 p_2 = 0$. Suppose one of the λ's, say λ_1, is zero. Thus we have $\lambda_2 p_2 = 0$, which implies that p_1 must be zero which is impossible. Otherwise, since λ_1 and λ_2 are not zero, then $p_1 = -(\lambda_2/\lambda_1) p_2$ which by definition, shows that p_1 and p_2 are not distinct. Hence, any two distinct points are linearly independent.

Now consider k points $p_1, p_2, \ldots, p_k$, which are linearly independent and hence determine a P.G.(k,p^n). Let p_{k+1} be any point not contained in the P.G.(k,p^n). We shall prove that p_1, $p_2, \ldots, p_k, p_{k+1}$ are linearly independent. Assume that they are linearly dependent. Then there exist $\lambda_1, \lambda_2, \ldots, \lambda_k, \lambda_{k+1}$, not all zero such that

$$\lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_k p_k + \lambda_{k+1} p_{k+1} = 0.$$

But $\lambda_{k+1} \neq 0$, since otherwise $p_1, p_2, \ldots, p_k$ would be linearly dependent. Hence

$$p_{k+1} = -\frac{\lambda_1}{\lambda_{k+1}} p_1 - \frac{\lambda_2}{\lambda_{k+1}} p_2 - \cdots - \frac{\lambda_k}{\lambda_{k+1}} p_k$$

and since $p_{k+1} \neq 0$, the $(\lambda_i / \lambda_{k+1})$'s are not all zero and thus p_{k+1} lies in the P.G.(k,p^n) which is impossible. Hence $p_1, p_2, \ldots, p_{k+1}$ are linearly independent and thus determine a P.G.$(k+1,p^n)$.

Next, we compute the number of P.G.(k,p^n)'s contained in P.G.(m,p^n). Every P.G.(k,p^n) is determined by a set of $k+1$ independent points. The first point, say p_1, may be chosen in $1+p^n+\ldots+p^{mn}$ ways. Next, p_2 may be chosen in the remaining $p^n+p^{2n}+\ldots+p^{mn}$ ways. The number of points on the line through p_1 and p_2, from previous work, is p^n+1. Thus the number of choices remaining for p_3, not on the line through p_1 and p_2, is $p^{2n}+p^{3n}+\ldots+p^{mn}$. After the ℓ th point has been chosen, where $\ell < k+1$, the $(\ell+1)$th point may be chosen from all the points not in the P.G.$(\ell-1,p^n)$, which is determined by $p_1, p_2, \ldots, p_\ell$. But the P.G.$(\ell-1,p^n)$ contains $1+p^n+p^{2n}+\ldots+p^{(\ell-1)n}$ points. This leaves $p^{\ell n}+p^{(\ell+1)n}+\ldots+p^{mn}$ choices for the $(\ell+1)$th point. Proceeding in this manner, the number of distinct ordered sets of $k+1$ independent points in the P.G.(m,p^n) is

$$(2.1) \qquad (1+p^n+\ldots+p^{mn})(p^n+p^{2n}+\ldots+p^{mn})\ldots(p^{kn}+p^{(k+1)n}+\ldots+p^{mn}).$$

From (2.1) the number of ordered sets of $k+1$ independent points in the P.G.(k,p^n) is given by

$$(1+p^n+\ldots+p^{kn})(p^n+p^{2n}+\ldots+p^{kn})\ldots(p^{(k-1)n}+p^{kn})p^{kn}.$$

Multiplying the above number by the number of P.G.(k,p^n)'s in our P.G.(m,p^n) we obtain the number in (2.1). Thus the number of P.G.

(k,p^n)'s contained in the P.G.(m,p^n) is

$$\frac{(1+p^n+\ldots+p^{mn})(p^n+p^{2n}+\ldots+p^{mn})\ldots(p^{kn}+p^{(k+1)n}+\ldots+p^{mn})}{(1+p^n+\ldots+p^{kn})(p^n+p^{2n}+\ldots+p^{kn})\ldots(p^{(k-1)n}+p^{kn})p^{kn}}.$$

We want to find, finally, the number of P.G.(s,p^n)'s in the P.G. (m,p^n) which contain a given P.G.(k,p^n). First, choose a point p_{k+2} not contained in the given P.G.(k,p^n). This point, p_{k+2}, may be chosen in $p^{(k+1)n}+p^{(k+2)n}+\ldots+p^{mn}$ different ways. Similarly p_{k+3} may be chosen from the $p^{(k+2)n}+p^{(k+3)n}+\ldots+p^{mn}$ points that are not contained in the P.G.$(k+1,p^n)$ which contains p_{k+2} and the given P.G.(k,p^n). Following this argument through, we can obtain a P.G.(s,p^n) containing the given P.G.(k,p^n) in

$$(p^{(k+1)n}+p^{(k+2)n}+\ldots+p^{mn})(p^{(k+2)n}+p^{(k+3)n}+\ldots+p^{mn})\ldots(p^{sn}+p^{(s+1)n}+\ldots+p^{mn})$$

ways.

Consider a given P.G.(s,p^n) obtained in this way. The number of ways in which we can select $s+1$ linearly independent points from this P.G.(s,p^n), $k+1$ of which are a fixed set of linearly independent points from the P.G.(k,p^n), may be found by setting $m=s$ in the above formula giving us

$$(p^{(k+1)n}+p^{(k+2)n}+\ldots+p^{sn})(p^{(k+2)n}+p^{(k+3)n}+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}.$$

Thus for $k<s\leq m$ we must have

$$\frac{(p^{(k+1)n}+p^{(k+2)n}+\ldots+p^{mn})\ldots(p^{sn}+p^{(s+1)n}+\ldots+p^{mn})}{(p^{(k+1)n}+p^{(k+2)n}+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}}$$

different P.G.(s,p^n)'s in the P.G.(m,p^n) which contain a given P.G.(k,p^n).

Summarizing, we have:

(1) Every P.G.(m,p^n) contains exactly $1+p^n+\ldots+p^{mn}$ points.

(2) Every P.G.(m,p^n) contains exactly

$$\frac{(1+p^n+\ldots+p^{mn})\ldots(p^{kn}+\ldots+p^{mn})}{(1+p^n+\ldots+p^{kn})\ldots(p^{(k-1)n}+p^{kn})p^{kn}}$$ distinct P.G.(k,p^n)'s.

(3) Every P.G.(k,p^n) in P.G.(m,p^n) is contained in

$$\frac{(p^{(k+1)n}+\ldots+p^{mn})\ldots(p^{sn}+\ldots+p^{mn})}{(p^{(k+1)n}+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}}$$ distinct P.G.(s,p^n)'s

for $k<s\leq m$.

For $k=0,1$, in particular, we obtain:

A. Every point is contained in

$$r=\frac{(p^n+\ldots+p^{mn})\ldots(p^{sn}+\ldots+p^{mn})}{(p^n+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}}$$

distinct P.G.(s,p^n)'s of a P.G.(m,p^n) where $0<s\leq m$.

B. Every line is contained in

$$\lambda=\frac{(p^{2n}+\ldots+p^{mn})\ldots(p^{sn}+\ldots+p^{mn})}{(p^{2n}+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}}$$

distinct P.G.(s,p^n)'s for $1<s\leq m$.

Every P.G.(s,p^n) contains, with every pair of points, the whole line joining them. Hence every pair of points is contained in λ different P.G.(s,p^n)'s.

In the following theorem we identify points with varieties and the P.G.(s,p^n)'s with blocks.

Theorem 2.1: The P.G.(s,p^n)'s contained in a P.G.(m,p^n) form a balanced incomplete block design with the following parameters:

$$b=\frac{(1+p^n+\ldots+p^{mn})\ldots(p^{sn}+\ldots+p^{mn})}{(1+p^n+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}}=b(s,m,p^n),$$

which gives the number of blocks, i.e., the number of different P.G.(s,p^n)'s contained in the P.G.(m,p^n);

$$v = 1+p^n+\ldots+p^{mn} = v(m,p^n),$$

i.e., the number of varieties is equal to the total number of points in the P.G.(m,p^n);

$$k = 1+p^n+\ldots+p^{sn} = k(s,p^n),$$

i.e., the number of plots in one block is the number of points contained in the P.G.(s,p^n);

$$r = \frac{(p^n+\ldots+p^{mn})\ldots(p^{sn}+\ldots+p^{mn})}{(p^n+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}} = r(s,m,p^n),$$

i.e., the number of replications is equal to the number of points common to all the different P.G.(s,p^n)'s formed from a given P.G. (m,p^n);

$$\lambda = \begin{cases} 1 \text{ if } s = 1, \\ \dfrac{(p^{2n}+\ldots+p^{mn})\ldots(p^{sn}+\ldots+p^{mn})}{(p^{2n}+\ldots+p^{sn})\ldots(p^{(s-1)n}+p^{sn})p^{sn}} \\ = \lambda(s,m,p^n) \text{ if } 1 < s \leq m, \end{cases}$$

where λ is the number of times two points of the P.G.(m,p^n) occur in pairs in different blocks. In the case where $s=1$, the blocks are the lines of the P.G.(m,p^n).

We shall prove that any P.G.(s,p^n) is either contained in a given P.G.$(m-1,p^n)$ or has a P.G.$(s-1,p^n)$ in common with it. Consider a P.G.(s,p^n) which is not contained in the P.G.$(m-1,p^n)$. Let p_1 be a point of the P.G.(s,p^n) which is not in the P.G.$(m-1, p^n)$. Let $q_1,\ldots,q_m,p_1$ be linearly independent points in the P.G.$(m-1,p^n)$. Then $q_1,\ldots,q_m,p_1$ are $m+1$ linearly independent points and hence every point of the P.G.(m,p^n) is of the form

$$\lambda_1 p_1 + \lambda_2 q_1 + \cdots + \lambda_{m+1} q_m .$$

Let $s+1$ linearly independent points of the P.G.(s,p^n) be $p_1, p_2, \ldots, p_{s+1}$. Since every point in the P.G.(s,p^n) is contained in the P.G.(m,p^n) and since every point in the P.G.(m,p^n) may be expressed in terms of the above $m+1$ linearly independent points, we have

$$p_i = \lambda_1^{(i)} p_1 + \lambda_2^{(i)} q_1 + \cdots + \lambda_{m+1}^{(i)} q_m , \quad i = 2,3,\ldots,s+1. \tag{2.2}$$

Hence the points $p_i' = p_i - \lambda_1^{(i)} p_1$, $i = 2,3,\ldots,s+1$, are contained in the P.G.$(m-1,p^n)$.

The points $p_2', p_3', \ldots, p_{s+1}'$ are now shown to be linearly independent. Suppose that they are linearly dependent. Then there must be a relation

$$\lambda_1 p_2' + \lambda_2 p_3' + \cdots + \lambda_s p_{s+1}' = 0 \tag{2.3}$$

where not all the λ_i's $= 0$. From (2.2) and (2.3) we have

$$\sum_{i=1}^{s} \lambda_i p_{i+1}' = \sum_{i=1}^{s} \lambda_i (p_{i+1} - \lambda_1^{(i+1)} p_1) , \tag{2.4}$$

$$\sum_{i=1}^{s} \lambda_i p_{i+1} - p_1 \sum_{i=1}^{s} \lambda_i \lambda_1^{(i+1)} = 0.$$

But $p_1, p_2, \ldots, p_{s+1}$ are linearly independent points. Hence (2.4) holds true only if all the coefficients of the p_i's in (2.4) are zero. This is true only if $\lambda_1 = \lambda_2 = \cdots = \lambda_s = 0$. Thus we see that $p_2', p_3', \ldots, p_{s+1}'$ are linearly independent. Hence the P.G.$(s-1, p^n)$ consisting of points of the form

$$\lambda_2 p_2' + \cdots + \lambda_{s+1} p_{s+1}', \tag{2.5}$$

is contained in the P.G.$(m-1,p^n)$. But these points are also all the points of the given P.G.(s,p^n) which are contained in the P.G. $(m-1,p^n)$. For suppose that there is another point p_1' of the P.G.

(s,p^n) contained in the P.G.$(m-1,p^n)$ and which is linearly independent of the points $p_2',\ldots,p_{s+1}'$. Then all the points of the P.G.(s,p^n) could be represented by

$$\gamma_1 p_1' + \gamma_2 p_2' + \cdots + \gamma_{s+1} p_{s+1}' ,$$

and would be in the P.G.$(m-1,p^n)$ contrary to our original assumption.

Thus every P.G.(s,p^n) of the P.G.(m,p^n) is either entirely contained in a given P.G.$(m-1,p^n)$ or has a P.G.$(s-1,p^n)$ in common with it.

Considering a P.G.(m,p^n) and deleting any given P.G.$(m-1,p^n)$ we obtain another system of points and lines which is called the finite Euclidean Geometry E.G.(m,p^n) of m dimensions. Considering a P.G.(s,p^n) which is not wholly contained in the P.G. $m-1,p^n)$, a P.G.$(s-1,p^n)$ is removed from the P.G.(s,p^n) turning it into a E.G.(s,p^n).

The number of points contained in an E.G.(m,p^n) is determined by taking the number of points in a P.G.(m,p^n) and removing from these all the points common to a P.G.$(m-1,p^n)$, i.e.,

$$v(m,p^n)-v(m-1,p^n) = p^{mn}.$$

The number of E.G.(s,p^n)'s contained in an E.G.(m,p^n) is determined by finding the number of P.G.(s,p^n)'s contained in a P.G.(m,p^n) which is $b(s,m,p^n)$. From this number we next delete the number of P.G.(s,p^n)'s contained in a P.G.$(m-1,p^n)$ which is $b(s,m-1,p^n)$. For, to form an E.G.(m,p^n) we delete a P.G.$(m-1,p^n)$ from the P.G.(m,p^n) which in turn deletes $b(s,m-1,p^n)$ P.G.(s,p^n)'s from the P.G.(m,p^n). This leaves $b(s,m,p^n)-b(s,m-1,p^n)$ P.G.(s,p^n)'s from which a P.G.$(s-1,p^n)$ is removed forming a E.G.(s,p^n). Hence

an E.G.(m,p^n) contains $b(s,m,p^n)-b(s,m-1,p^n)$ E.G.(s,p^n)'s.

Consider a given E.G.(k,p^n), $k<s$. It arose from a P.G.(k,p^n) contained in the P.G.(m,p^n) but not wholly contained in the P.G.$(m-1,p^n)$. The P.G.(k,p^n) is contained in a certain number, say c, of P.G.(s,p^n)'s. Since the given P.G.(k,p^n) is not wholly contained in the P.G.$(m-1,p^n)$ then neither are the P.G.(s,p^n)'s which contain it. When the P.G.$(m-1,p^n)$ is removed the P.G.(k,p^n) becomes an E.G.(s,p^n) and all the P.G.(s,p^n)'s become E.G.(s,p^n)'s containing the given E.G.(k,p^n). Hence the number of E.G.(s,p^n)'s containing a given E.G.(k,p^n) is the same as the number of P.G.(s,p^n)'s containing a given P.G.(k,p^n). We now have

Theorem 2.2: The E.G.(s,p^n)'s contained in an E.G.(m,p^n) form a balanced incomplete block design with the following parameters:

$b = b(s,m,p^n)-b(s,m-1,p^n)$, since the E.G.$(s,p^n)$'s represent blocks;

$v = p^{mn}$, since the points of the E.G.(m,p^n) represent varieties;

$k = p^{sn}$, since the points in an E.G.(s,p^n) represent plots;

$r = r(s,m,p^n)$;

$\lambda = \lambda(s,m,p^n)$.

To establish the last two equalities we consider the following argument.

Consider a point contained in the E.G.(m,p^n). This point was also in the P.G.(m,p^n) and, from previous work, was in

$r(s,m,p^n)$P.G.(s,p^n)'s. Since the point is in the E.G.(m,p^n) it was not in the P.G.$(m-1,p^n)$ which was deleted from the P.G.(m,p^n). Hence all the P.G.(s,p^n)'s which contained that point were not wholly contained in the P.G.$(m-1,p^n)$ and hence are carried over into $r(s,m,p^n)$ E.G.(s,p^n)'s containing that point. Thus, the number of times that every point is contained in different E.G. (s,p^n)'s is $r(s,m,p^n)$.

Finally, $\lambda(s,m,p^n)$ is the number of times a given pair of points, p_1 and p_2, say, appear in different P.G.(s,p^n)'s. After the P.G.$(m-1,p^n)$ has been removed, either p_1,p_2 are not contained in the E.G.(m,p^n) or they appear together in the E.G.(s,p^n)'s derived from the P.G.(s,p^n)'s which contain them. Hence every pair of points in the E.G.(m,p^n) is contained in exactly $\lambda(s,m,p^n)$ F.G.(s,p^n)'s.

As an illustration we shall form the lines of the P.G. (3,2) and the E.G.(3,2). Every line of the P.G.(3,2) forms a P.G.(1,2). The number of points contained in a P.G.(1,2), by an earlier theorem, is $1+2=3$. Hence every line of the P.G.(3,2) contains three points. This can be seen also by forming all possible combinations of $\lambda_1 p_1 + \lambda_2 p_2$., where p_1 and p_2 are distinct points and λ_1, λ_2 form all possible non-proportional pairs of the G.F.(2) where λ_1 and λ_2 are not both zero. The number of points in the P.G.(3,2) is 15. The number of lines contained in the P.G.(3,2) is 35. To find the number of lines containing a given point corresponds to finding the number of P.G.(1,2)'s in the P.G.(3,2) that contain the given point. This is seen to be

$$r=(2+2^2+2^3)/2=7.$$

The E.G.(3,2) contains $2^3=8$ points. The number of points on each line of an E.G.(3,2) is two. Hence the number of lines in the E.G.(3,2) is ${}_8C_2=28$. The number of lines on which a point appears in an E.G.(1,2) is the same as finding the number of times a point appears in an P.G.(1,2) which, from above, is seven.

Hence we form the incomplete balanced block designs with the following parameters:

$b=35 \quad v=15 \quad r=7 \quad k=3 \quad \lambda=1$,

$b=28 \quad v=8 \quad r=7 \quad k=2 \quad \lambda=1$.

The G.F.(2) consisting of the elements 0,1 is the field used in obtaining all the points of the P.G.(3,2). Thus we have the following points:

$p_1=1000, \quad p_5=1100, \quad p_9=0101, \quad p_{13}=1011,$

$p_2=0100, \quad p_6=1010, \quad p_{10}=0011, \quad p_{14}=0111,$

$p_3=0010, \quad p_7=1001, \quad p_{11}=1110, \quad p_{15}=1111.$

$p_4=0001, \quad p_8=0110, \quad p_{12}=1101,$

Taking all pairs of distinct points in the P.G.(3,2) and forming all possible combinations of the form $\lambda_1 p_1+\lambda_2 p_2$ where (λ_1,λ_2) consists of all pairs of points of the G.F.(2) where at least one λ is not zero,i.e.,

$$(\lambda_1,\lambda_2)=(0,1),\ (1,0),\ (1,1);$$

we thus form all the lines contained in the P.G.(3,2). From this we see, for example, that p_1,p_2, and $p_5=p_1+p_2$ are the three points on the line through p_1,p_2. Hence, if any two of p_1,p_2,p_5 are given, the line through the two given points determines the third point. Working in a systematical manner the lines of the

P.G.(3,2) are the following:

$p_1p_2p_5$, $p_2p_3p_8$, $p_3p_5p_{11}$, $p_4p_{11}p_{15}$, $p_6p_{12}p_{14}$,
$p_1p_3p_6$, $p_2p_4p_9$, $p_3p_7p_{13}$, $p_5p_6p_8$, $p_7p_8p_{15}$,
$p_1p_4p_7$, $p_2p_6p_{11}$, $p_3p_9p_{14}$, $p_5p_7p_9$, $p_7p_{11}p_{14}$,
$p_1p_8p_{11}$, $p_2p_7p_{12}$, $p_3p_{12}p_{15}$ $p_5p_{10}p_{15}$, p_8p_9 p_{10},
$p_1p_9p_{12}$, $p_2p_{10}p_{14}$, $p_4p_5p_{12}$, $p_5p_{13}p_{14}$, $p_8p_{12}p_{13}$,
$p_1p_{10}p_{13}$, $p_2p_{13}p_{15}$, $p_4p_6p_{13}$, $p_6p_7p_{10}$, $p_9p_{11}p_{13}$,
$p_1p_{14}p_{15}$, $p_3p_4p_{10}$, $p_4p_8p_{14}$, p_6p_9 p_{15}, $p_{10}p_{11}p_{12}$.

To form an E.G.(3,2) we must delete a P.G.(2,2) from the P.G.(3,2). Every line of the P.G.(2,2) contains three points. Also a P.G.(2,2) contains $1+2+2^2=7$ points. Since p_1,p_2,p_3 are three linearly independent points, they generate a P.G.(2,2) contained in the P.G.(3,2). Thus, in forming an E.G.(3,2), we must remove a set of seven points which is determined by forming all possible combinations of $\lambda_1p_1+\lambda_2p_2+\lambda_3p_3$ where at least one of the λ's is not zero. The set of points obtained in this manner is $p_1,p_2,p_3,p_5,p_6,p_8,p_{11}$. It should be noted that this set of points forming a P.G.(2,2) is that set of points formed by choosing the points whose last coordinate is zero. This is possible since this set of points is closed under addition.

Since the lines of the E.G.(3,2) contain two points then the total number of combinations of pairs of the remaining 28 points represent all the lines in the E.G.(3,2). They are as follows:

p_4p_7 , p_4p_{10}, p_4p_{13}, p_4p_{15}, p_7p_9,
p_4p_9 , p_4p_{12}, p_4p_{14}, p_7p_9, p_7p_{10},

p_7p_{12}, p_9p_{15}, p_9p_{14}, $p_{10}p_{15}$, $p_{13}p_{15}$,
p_7p_{13}, p_9p_{10}, $p_{10}p_{12}$, $p_{12}p_{13}$, $p_{14}p_{15}$.
p_7p_{14}, p_9p_{12}, $p_{10}p_{13}$, $p_{12}p_{14}$,
p_7p_{15}, p_9p_{13}, $p_{10}p_{14}$, $p_{12}p_{15}$,

Notice that each point in the E.G.(3,2) appears in exactly seven lines as did each point in the P.G.(3,2).

As an example of a finite Euclidean geometry we now construct the E.G.(2,3). The P.G.(2,3) has $1+3+3^2=13$ points. The E.G.(2,3) has $3^2=9$ points. Forming the 13 distinct points, we have

$p_1=(1,0,0)$, $p_5=(1,0,1)$, $p_9=(1,0,-1)$,
$p_2=(0,1,0)$, $p_6=(0,1,1)$, $p_{10}=(-1,1,1)$,
$p_3=(0,0,1)$, $p_7=(1,1,1)$, $p_{11}=(1,-1,1)$,
$p_4=(1,1,0)$, $p_8=(1,-1,0)$, $p_{12}=(1,1,-1)$,
$p_{13}=(0,-1,1)$.

The number of points in a line is the number of points contained in a P.G.(1,3) which is four. The line through p_1,p_2 is of the form $\lambda_1p_1+\lambda_2p_2$ and contains the points p_1,p_2,p_4,p_8 for (λ_1,λ_2) equal to $(1,0),(0,1),(1,1)$, and $(1,-1)$ respectively. In a systematic fashion we obtain the $r(1,2,3)=13$ lines of the P.G.(2,3), viz.,

$p_1p_2p_4p_8$, $p_2p_3p_6p_{13}$, $p_3p_8p_{10}p_{11}$,
$p_1p_3p_5p_9$, $p_2p_5p_7p_{11}$, $p_4p_5p_{10}p_{13}$,
$p_1p_6p_7p_{10}$, $p_2p_9p_{10}p_{12}$, $p_4p_6p_9p_{11}$, $p_7p_8p_9p_{13}$.
$p_1p_{11}p_{12}p_{13}$, $p_3p_4p_7p_{12}$, $p_5p_6p_8p_{12}$,

Now from the P.G.(2,3) delete a P.G.(1,3) forming an E.G.(2,3) which contains $3^2 = 9$ points. But any P.G.(1,3) is a line in the P.G.(2,3) containing four points. Thus, by deleting any line, say $p_1p_2p_4p_8$, the remaining nine points form an E.G.(2,3). Since every line contained in the E.G.(2,3) has three points, and since there are $b(1,2,3)-b(1,1,3) = 12$ lines in the E.G.(2,3), we have, as the lines of the E.G.(2,3), the following:

$$p_3p_5p_9, \quad p_3p_6p_{13}, \quad p_3p_7p_{12}, \quad p_6p_9p_{11},$$
$$p_6p_7p_{10}, \quad p_5p_7p_{11}, \quad p_3p_{10}p_{11}, \quad p_5p_6p_{12},$$
$$p_{11}p_{12}p_{13}, \quad p_9p_{10}p_{12}, \quad p_5p_{10}p_{13}, \quad p_7p_9p_{13}.$$

The above system of nine points and twelve lines is the E.G.(2,3).

An E.G.$(2,p^n)$ may be constructed in another way using a set of orthogonal Latin squares. From the previous chapter we have shown that it is possible to construct p^n-1 orthogonal Latin squares from a Galois field of order p^n, where p is a prime. Since the Latin squares have side p^n, the number of compartments in each Latin square is p^{2n}. From the set of orthogonal Latin squares we can form p^{2n} sets of ordered numbers $(a_{ij1}, a_{ij2}, \ldots, a_{ij,p^n-1})$ where a_{ijk} is the number in the $\underline{i}$th row and $\underline{j}$th column of the $\underline{k}$th Latin square. These sets of numbers are arranged in a square where the above general set would appear in the $\underline{i}$th row and $\underline{j}$th column. These sets are then called the points of our E.G.$(2,p^n)$ and are p^{2n} in number. The lines of the E.G.$(2,p^n)$ are then given by the columns, the rows, and by the (p^n-1) sets of points whose $\underline{i}$th number is α $(\alpha = 0,1,\ldots,p^n-1; i = 1,2,\ldots,p^n-1)$. The p^n+1 sets of lines obtained in this way are called parallel lines since no two lines in a given set have a point in common. Each set contains

p^n lines so that all together $p^n(p^n+1)$ lines are obtained.

As an illustration consider the E.G.(2,3). The two orthogonal Latin squares formed from the G.F.(3) are

$$\begin{array}{ccc} 0 & 1 & 2 \\ 1 & 2 & 0 \\ 2 & 0 & 1 \end{array} \qquad \begin{array}{ccc} 0 & 1 & 2 \\ 2 & 0 & 1 \\ 1 & 2 & 0 \end{array}.$$

Superimposing the second upon the first we obtain the following set of points:

$$\begin{array}{ccc} (0,0) & (1,1) & (2,2) \\ (1,2) & (2,0) & (0,1) \\ (2,1) & (0,2) & (1,0). \end{array}$$

In order to illustrate the above argument more clearly we shall label the above set of points in their respective positions as follows:

$$\begin{array}{ccc} p_3 & p_5 & p_9 \\ p_6 & p_7 & p_{10} \\ p_{13} & p_{11} & p_{12}. \end{array}$$

The points are labelled in the above manner in order to simplify the comparision with the results obtained earlier. The rows and the columns give the following set of lines respectively:

$$\begin{array}{lll} p_3\ p_{10} p_{11} & & p_3\ p_7\ p_{12} \\ p_5\ p_6\ p_{12} & & p_5\ p_{10} p_{13} \\ p_7\ p_9\ p_{13} & & p_6\ p_9\ p_{11}. \end{array}$$

These are the same lines as obtained in our first construction of an E.G.(2,3).

In order to extend this E.G.$(2,p^n)$ to form the P.G.$(2,p^n)$

we must add additional points, the same point to each set of parallel lines and different points to intersecting lines. Finally we take all the points that were added and form an additional line through them.

Returning to our example, we see that in order to form the P.G.(2,3), we must add p_1 to the first set, p_2 to the second, p_8 to the third set, and p_4 to the fourth set. In addition, add the line $p_1p_2p_8p_4$. Thus, the resulting P.G.(2,3) has 13 lines of the P.G.(2,3) which we have labelled in the same manner as the 13 lines of the P.G.(2,3) in the previous example.

An E.G.$(2,p^n)$ has p^{2n} points. So does the design whose construction we have described. The number of lines in an E.G. $(2,p^n)$ is the number of E.G.$(1,p^n)$'s contained in it which is, for $s=1$,

$$b(1,2,p^n)-b(1,1,p^n) = \frac{(1+p^n+p^{2n})(p^n+p^{2n})}{(1+p^n)p^n} = \frac{(1+p^n)p^n}{(1+p^n)p^n} = p^n(p^n+1),$$

and our design has this property also.

The number of times a point appears on a line in an E.G. $(2,p^n)$ is, for $s=1$ and $m=2$

$$r(1,2,p^n) = \frac{(p^n+p^{2n})}{p^n} = 1+p^n.$$

This holds for our design since every point appears once and only once in a set of parallel lines and we have $1+p^n$ such sets.

The number of times that a pair of points appear together on an E.G.$(1,p^n)$, or line, in an E.G.$(2,p^n)$ is

$$\lambda = \lambda(1,2,p^n) = 1.$$

We shall show that our design has this property. Consider any pair of points. If the two points are in a row they lie on one row line and one no other line. A similar remark applies if they lie in a column. Suppose the points lie on two lines which are neither row nor column lines. One of these lines will arise from some fixed $i = i_1$ and $\alpha = \alpha_1$; the other from $i = i_2, \alpha = \alpha_2$. This means that the two ordered sets of numbers which are our points would both have α_1 in the i_1th place and α_2 in the i_2nd place. This is impossible since, from the definition of orthogonal Latin squares every ordered pair of numbers from the set $0,1,\ldots,p^n-1$ appears in these positions once and only once.

Thus the alternative approach does lead to an E.G.$(2,p^n)$.

Finite geometries furnish whole series of balanced incomplete block designs. Most of these designs are of little practical interest since the number of replications should, in most cases, not exceed ten.

By applying two theorems first proved by R.C.Bose (Annals of Eugenics,9 (1939) pp. 358-399), other series of these designs can be obtained. Before proceeding to these theorems we must first introduce the concept of a module. A module is a system of elements such that to each pair of elements,a,b, there is uniquely defined a sum a+b satisfying the postulates I,II,III,IV, for addition in a field. For example, the residues mod m form a module for every m. A module,M, with a finite number of elements is called a finite module. If M has n elements then M is called a module of order n.

Let M now be a module of order n and let m varieties $A_1^{(i)}, \ldots, A_m^{(i)}$, $i = 1, \ldots, n$, correspond to every element $A^{(i)}$ of the module. We form blocks of these mn varieties as follows:

$$(A_{i_1}^{(\alpha_1)}, \ldots, A_{i_k}^{(\alpha_k)}), (A_j^{(\beta_1)}, \ldots, A_j^{(\beta_k)}), \ldots,$$

where the varieties in a block are distinct but not necessarily so in different blocks.

As an illustration consider the module consisting of the elements 0,1,2,3,4 which are added together in the usual fashion, the resulting sums being reduced modulo 5. In the case where the number of varieties corresponding to every element in the module is two, we have the following varieties: $0_1, 0_2, 1_1, 1_2, 2_1, 2_2, 3_1, 3_2, 4_1, 4_2$. Taking $k = 3$, we can form the following blocks from the above module:

$$(0_1, 1_2, 2_1), \quad (0_2, 3_1, 4_2).$$

Given a block of k varieties we can write $k P 2 = k(k-1)$ expressions of the form

$$A_\gamma - B_\delta = (A-B)_{\gamma\delta}$$

where A and B are any two varieties in the block. This expression is called a difference of type $\gamma\delta$.

From our example computing the differences for $(0_1, 1_2, 2_1)$ we have

$$0_1 - 1_2 = (0-1)_{12} = 4_{12} \ (5),$$
$$0_1 - 2_1 = (0-2)_{11} = 3_{11} \ (5),$$
$$1_2 - 0_1 = (1-0)_{21} = 1_{21} \ (5),$$
$$1_2 - 2_1 = (1-2)_{21} = 4_{21} \ (5),$$
$$2_1 - 0_1 = (2-0)_{11} = 2_{11} \ (5),$$
$$2_1 - 1_2 = (2-1)_{12} = 1_{12} \ (5).$$

The differences for $(0_2,3_1,4_2)$ are the following:

$$0_2-3_1 = 2_{21},$$
$$0_2-4_2 = 1_{22},$$
$$3_1-0_2 = 3_{12},$$
$$4_2-0_2 = 4_{22},$$
$$4_2-3_1 = 1_{21},$$
$$3_1-4_2 = 4_{12}.$$

Differences of the type $\alpha\beta$, say $A_{\alpha\beta}$, are called pure if $\alpha=\beta$ and are called mixed if $\alpha\neq\beta$.

If, in t blocks, every pure difference, $A_{\alpha\alpha}$, except $0_{\alpha\alpha}$ is repeated λ times and every mixed difference, $A_{\alpha\beta}$, is repeated the same number of times, including $0_{\alpha\beta}$, the differences are said to be symmetrically repeated.

Theorem 2.3: Let M be a module containing the elements $v^{(0)},\ldots,v^{(n-1)}$, and let m varieties $v_1^{(i)},\ldots,v_m^{(i)}$ correspond to every element $v^{(i)}$. The variety v_j is said to belong to the jth class. Suppose that there exist t blocks of elements $B_1,\ldots,B_t$, not necessarily containing the same number of elements, such that:

(1) No two varieties appearing in the same block are alike. However, the same variety may appear in different blocks.

(2) Among the elements in $B_1,B_2,\ldots,B_t$ exactly r varieties belong to each of the m classes.

(3) The differences formed from $B_1,B_2,\ldots,B_t$ are symmetrically repeated, each occurring λ times.

Also if

$$B_i = (v_{\alpha_1}^{(i_1)},\ldots,v_{\alpha_k}^{(i_k)})$$

is any one of the blocks $B_1,B_2,\ldots,B_k$ and $v^{ie}+\theta=v^{je}$ let

$$B_{i\theta} = (v_{\alpha_1}^{(i_1)}, \ldots, v_{\alpha_k}^{(i_k)}).$$

Form all the blocks B_i for all i and all θ contained in M. Then

A. In the blocks $B_{i\theta}$ every variety occurs r times.

B. Any two varieties occur together in the same block exactly λ times.

Proof of Theorem 2.3: Corresponding to every pair of elements $v^{(\alpha)}$ and $v^{(\beta)}$ of M there exists exactly one θ in M such that $v^{(\alpha)} + \theta = v^{(\beta)}$. This relation is valid since every non-zero element in a module has an inverse.

From the r varieties belonging to the ith class, take one and add all possible values of θ to it. This will give all the varieties with subscript i exactly once. Thus, working with the r varieties belonging to the ith class, we obtain each variety in the ith class r times. Hence, considering all values of i we obtain every variety in each class exactly r times.

Every pair of varieties, $v_\alpha^{(i)}$ and $v_\beta^{(j)}$, where α may be equal to β or i equal to j but both equalities not holding together, occur together exactly μ times in the blocks B_i if and only if there exist exactly μ blocks in the $B_1, \ldots, B_t$ each containing a pair of elements $v_\alpha^{(i')}$, $v_\beta^{(j')}$ and, corresponding to each such pair, there exists an element θ of the module such that

$$v^{(i')} + \theta = v^{(i)},$$
$$v^{(j')} + \theta = v^{(j)}.$$

Thus $v^{(i')} - v^{(j')} = v^{(i)} - v^{(j)} = d$ and $\theta = v^{(i)} - v^{(i')} = v^{(j)} - v^{(j')}$. Hence the pair $v_\alpha^{(i)}, v_\beta^{(j)}$ arises exactly as many times as the difference d arises as a difference of the type $\alpha\beta$ in the original blocks. If $\alpha = \beta$, this implies that $i' \neq j'$. Hence $v_\alpha^{(i')} - v_\beta^{(j')} = d_{\alpha\beta}$ is not a difference

of the type $O_{\alpha\alpha}$ and the number of $d_{\alpha\alpha}$'s is λ by hypothesis. If $\alpha \neq \beta$, $v_\alpha^{(i')} - v_\beta^{(j')} = d_{\alpha\beta}$ may be of the type $O_{\alpha\beta}$ but whether it is or not there are exactly λ such differences by hypothesis. Hence $\mu = \lambda$.

Corollary to Theorem 2.3: If each block B_i contains the same number of varieties the blocks B_i form an incomplete balanced block design with $v = mn$, $b = nt$ and r, k, λ, as in the theorem.

As an example consider the group of residues mod $2t+1$ and the pairs

$$(1,2t),\ (2,2t-1),\ \ldots,\ (t,t+1).$$

Every difference different from zero arises from these pairs exactly once. Next, consider the blocks

$$(1_1,(2t)_1,0_2),\ (2_1,(2t-1)_1,0_2),\ \ldots,\ (t_1,(t+1)_1,0_2);$$

$$(1_2,(2t)_2,0_3),\ (2_2,(2t-1)_2,0_3),\ \ldots,\ (t_2,(t+1)_2,0_3);$$

$$(1_3,(2t)_3,0_1),\ (2_3,(2t-1)_3,0_1),\ \ldots,(t_3,(t+1)_3,0_1);$$

$$(0_1,0_2,0_3).$$

From the first two elements of the first $3t$ blocks we obtain all the pure differences exactly once. All non-zero mixed differences of types 1,2 and 2,1 arise exactly once from the first set of t blocks, those of types 2,3, and 3,2 exactly once from the second set of t blocks, and those of types 1,3 and 3,1 exactly once from the third set of blocks. The zero mixed differences arise exactly once from the block $(0_1,0_2,0_3)$. The system of blocks formed above contains $6t+3$ varieties, three in each block. When we form the $B_{1\theta}$'s, θ may take on any of the $2t+1$

values $0,1,2,\ldots,2t$ leading to $(3t+1)(2t+1)$ blocks. The original set of blocks has $3t+1$ elements in each of the classes 1,2, and 3. From Theorem 2.3 we can construct an incomplete balanced block design with the example above with the parameters $v=6t+3$, $b=(3t+1)(2t+1)$, $r=3t+1$, $k=3$, $\lambda=1$.

For example, put $t=2$, then $2t+1=5$. Arranging the initial blocks in the first row and forming each successive row of blocks by adding 1,2,3,4 as the values of θ respectively we have the following design consisting of 35 blocks:

$(1_1,4_1,0_2)$ $(2_1,3_1,0_2)$ $(1_2,4_2,0_3)$ $(2_2,3_2,0_3)$ $(1_3,4_3,0_1)$ $(2_3,3_3,0_1)$ $(0_1,0_2,0_3)$

$(2_1,0_1,1_2)$ $(3_1,4_1,1_2)$ $(2_2,0_2,1_3)$ $(3_2,4_2,1_3)$ $(2_3,0_3,1_1)$ $(3_3,4_3,1_1)$ $(1_1,1_2,1_3)$

$(3_1,1_1,2_2)$ $(4_1,0_1,2_2)$ $(3_2,1_2,2_3)$ $(4_2,0_2,2_3)$ $(3_3,1_3,2_1)$ $(4_3,0_3,2_1)$ $(2_1,2_2,2_3)$

$(4_1,2_1,3_2)$ $(0_1,1_1,3_2)$ $(4_2,2_2,3_3)$ $(0_2,1_2,3_3)$ $(4_3,2_3,3_1)$ $(0_3,1_3,3_1)$ $(3_1,3_2,3_3)$

$(0_1,3_1,4_2)$ $(1_1,2_1,4_2)$ $(0_2,3_2,4_3)$ $(1_2,2_2,4_3)$ $(0_3,3_3,4_1)$ $(1_3,2_3,4_1)$ $(4_1,4_2,4_3)$.

Notice that in the above 35 blocks each variety occurs seven times and every pair of varieties is repeated exactly once.

To the module M adjoin the symbol ∞ which obeys the following rule under addition. For every element a contained in M $\infty+a=\infty$.

Theorem 2.4: Let M be a module with the n elements $u^{(0)}$, $u^{(1)},\ldots,u^{(n-1)}$. To every element $u^{(\infty)}$ there corresponds m varieties

$u_1^{(\alpha)}, u_2^{(\alpha)},\ldots,u_m^{(\alpha)}$. One variety corresponds to the element ∞. The variety $u_i^{(\alpha)}$ belongs to the ith class and the $u_i^{(\alpha)}$'s are said to be finite varieties for all i and all α. Suppose there exist t+s blocks $B_1,\ldots,B_t,B_1',\ldots,B_s'$ such that:

I The varieties in each block are different from each other.

II The blocks $B_1,\ldots,B_t$ contain exactly k finite varieties each and do not contain the element ∞ while $B_1',\ldots,B_s'$ contain exactly k-1 finite varieties and ∞.

III Among the varieties in $B_1,\ldots,B_t$ exactly ns-λ belong to each class, while among the varieties in $B_1',\ldots,B_s'$, exactly λ belong to each class.

IV The differences arising from the finite varieties are symmetrically repeated, each occurring λ times.

The blocks $B_{i\theta},B_{j\theta}'$ are defined as in the previous theorem.

Then the blocks $B_{i\theta},B_{j\theta}'$, $i=1,\ldots,t;j=1,\ldots,s$, form an incomplete balanced block design with the parameters $v=mn+1$, $b=n(t+s)$, $r=ns$, k,λ.

Proof: From III exactly ns-λ+λ varieties belong to each class. Thus, from Theorem 2.3, each variety occurs exactly ns times in the blocks $B_{i\theta},B_{j\theta}'$, and every pair of finite varieties occurs exactly λ times together in all the blocks $B_{i\theta},B_{j\theta}'$. The symbol ∞ appears exactly once in each of the $B_{j\theta}'$ blocks, $j=1,\ldots,s$. Hence the variety ∞ occurs also exactly ns times. Again, from III and Theorem 2.3, each variety in the $B_{j\theta}'$ occurs exactly λ times. Hence ∞ occurs with every finite variety λ times in the same block. Thus every pair of varieties, ∞ being considered

a variety, occur exactly λ times together in the blocks $B_{i\theta}, B'_{j\theta}$. Now applying the Corollary to Theorem 2.3 to the above argument the proof of Theorem 2.4 is complete.

As an example we shall construct designs with the parameters $v = 12t+4$, $b = (3t+1)(4t+1)$, $r = 4t+1$, $k = 4$, and $\lambda = 1$, where $4t+1$ is a power of a prime.

We take the elements of the G.F.$(4t+1)$ as our module M where addition is the operation involved. Let x be a primitive root. We shall now show that there exist odd numbers α and q such that $(x^{\alpha}+1)/(x^{\alpha}-1) = x^{q}$.

Since x is a primitive root the non-zero elements of the G.F.$(4t+1)$ are generated by different powers of x. These elements are given by $x^{0}, x^{1}, \ldots, x^{4t-1}$. We shall consider expressions of the form $(x^{\alpha}+1)/(x^{\alpha}-1)$. Since x is a primitive root of the G.F. $(4t+1)$ then $x^{4t} = 1$, i.e., $(x^{2t}-1)(x^{2t}+1) = 0$. Since $x^{2t} \neq 1$, then $x^{2t} = -1$. Since $x^{\alpha} \neq 1$ is a non-zero element in the G.F.$(4t+1)$ for $\alpha \neq 0, 2t$, and since every non-zero element in the field has a multiplicative inverse, we have

$$\frac{x^{\alpha}+1}{x^{\alpha}-1} = x^{q}, \text{ where } 1 \leq q \leq 4t-1, \tag{2.6}$$

and $\alpha = 1, 2, \ldots, 2t-1, \ldots, 4t-1$. From (2.6) $x^{\alpha} = (x^{q}+1)/(x^{q}-1)$. This relation is valid since $x^{q}-1$ is a non-zero element in the G.F.$(4t+1)$. Hence, to every $\alpha \neq 0, 2t$, there exists a unique value $q \neq 0, 2t$, and contained among the residues $1, 2, \ldots, 2t-1, \ldots, 4t-1$. Among these remaining residues there are 2t odd residues and 2t-2 even residues. Now α and q can be paired so that both are even residues, or one is even and the other odd, or both are

odd. In the extreme case, where either α is odd and q is even, or vice versa, we have two pairs of odd residues remaining after pairing α with q. Hence, to at least two odd residues, there corresponds an odd residue.

Now let three varieties correspond to each element of the G. F.$(4t+1)$. We form the following $3t+1$ blocks:

$$(x_1^{2i}, x_1^{2t+2i}, x_2^{2i+\alpha}, x_2^{2t+2i+\alpha});$$

$$(x_2^{2i}, x_2^{2t+2i}, x_3^{2i+\alpha}, x_3^{2t+2i+\alpha}); \quad i = 0,1,\ldots,t-1,$$

$$(x_3^{2i}, x_3^{2t+2i}, x_1^{2i+\alpha}, x_1^{2t+2i+\alpha});$$

$$(\infty, 0_1, 0_2, 0_3).$$

Now set $x^{\alpha}+1 = x^u$, $x^{\alpha}-1 = x^v$, $x^{2t}-1 = x^{\beta}$. Now α may be chosen so that

$$u - v \equiv 1 \ (2), \tag{2.7}$$

that is, so that q will be odd.

Each of the three classes of varieties occurs $4t$ times in the first $3t$ blocks and once in the last block. The differences of the type 1,1 occur in the first and third set of blocks. These differences may be written as

$$\left[x^{2i+2\epsilon_1 t+\epsilon_2\alpha}(x^{2t}-1)\right]_{11} = x_{11}^{2i+2\epsilon_1 t+\epsilon_2\alpha+\beta}, \quad (i = 0,1,\ldots,t-1), \tag{2.8}$$

where ϵ_1, ϵ_2 take on the values 0,1 independently. Hence (2.8) represents four differences of the type 1,1 for each value of i. Now suppose that two of these differences are equal. Then

$$x_{11}^{2i+\epsilon_1 2t+\epsilon_2\alpha+\beta} = x_{11}^{2j+\epsilon_1' 2t+\epsilon_2'\alpha+\beta}.$$

Therefore

$$x_{11}^{2(i-j)\ 2t(\epsilon_1-\epsilon_1')+\alpha(\epsilon_2-\epsilon_2')} = 1,$$

that is,

(2.9) $$2(i-j) + 2t(\epsilon_1 - \epsilon_1') \equiv -\alpha(\epsilon_2 - \epsilon_2') \quad (4t).$$

Since α is odd, (2.9) is valid if and only if $\epsilon_2 - \epsilon_2'$ is even, i.e., $\epsilon_2 \equiv \epsilon_2' \ (2)$. But both ϵ_2 and ϵ_2' are either 0 or 1. Hence ϵ_2 must be equal to ϵ_2'. Thus, from (2.9), since $\epsilon_1 - \epsilon_1'$ is equal to either 0 or ± 1 either $i-j \equiv 0 \ (2t)$ or $i-j \equiv t \ (2t)$. Since $i \neq j$ and $0 \leq i,j \leq t-1$, both of these congruences are impossible. Thus the $4t$ differences of type 1,1 are all distinct and different from zero. Therefore they must contain each of the $4t$ non-zero elements exactly once. The above argument may be applied to differences of the type 2,2 and 3,3 to show that they contain all the non-zero elements of the G.F.$(4t+1)$ exactly once.

Now consider mixed differences of the type 1,2. These differences occur in the first set of blocks and the last block only. The differences arising from the first set of blocks may be written as

(2.10) $$(x^{2i+\epsilon_1 2t} - x^{2i+\alpha+\epsilon_2 2t})_{12},$$

where ϵ_1, ϵ_2 again take on the values 0,1 independently. The four differences given by (2.10) are now written more explicitly as follows:

$$\left[-x^{2i}(x^{\alpha}-1)\right]_{12} = x_{12}^{2i+2t+v}, \quad \left[x^{2i}(x^{\alpha}-1)\right]_{12} = x_{12}^{2i+v},$$

$$\left[x^{2i}(x+1)\right]_{12} = x_{12}^{2i+u}, \quad \left[-x^{2i}(x^{\alpha}+1)\right]_{12} = x^{2i+2t+u}.$$

The above expressions may be condensed into the following forms, i.e., $x_{12}^{2i+\epsilon 2t+u}$, $x_{12}^{2i+\epsilon 2t+v}$, where $\epsilon = 0,1$. Thus (2.10) represents $4t$ non-zero elements of the G.F.$(4t+1)$. It remains to show now that these elements are distinct. Suppose that two of these diff-

erences are equal. There are two cases to be considered. Consider first

$$x_{12}^{2i+\epsilon 2t+u} = x_{12}^{2j+\epsilon' 2t+u} .$$

This implies that $2(i-j) + 2t(\epsilon - \epsilon') \equiv 0 \ (4t)$, that is, $i-j \equiv t(\epsilon - \epsilon') \ (2t)$ which has been shown to be impossible. Next, suppose that

$$x_{12}^{2i+\epsilon 2t+u} = x_{12}^{2j+\epsilon' 2t+v} . \tag{2.11}$$

Thus $2(i-j) + 2t(\epsilon - \epsilon') \equiv v-u \ (4t)$. From this we can conclude that $u-v \equiv 0 \ (2)$, but this is impossible since $u-v \equiv 1 \ (2)$. Thus (2.10) represents the $4t$ non-zero elements of the G.F.$(4t+1)$ exactly once. The proof for the other mixed differences is analogous. The zero mixed differences all arise from the last block. Thus all the conditions for Theorem 2.4 are satisfied. Hence we have an incomplete balanced block design with the following values for the parameters: $b = (3t+1)(4t+1)$, $v = 12t+3$, $r = 4t+1$, $k = 4$, $\lambda = 1$.

As an illustration let $4t+1 = 9$. From the Corollary to Theorem 1.5, the G.F.(3^2) may be expressed as the field of residues mod $(3, y^2+1)$. The set of residues is thus $0, 1, -1, y, -y, y+1, -y-1, y-1, -y+1$. We see that $x = -y+1$ is a primitive root, for

$$\begin{aligned} x^2 &= y, & x^6 &= -y, \\ x^3 &= y+1, & x^7 &= -y-1, \\ x^4 &= -1, & x^8 &= 1, \\ x^5 &= y-1, \end{aligned}$$

where the values for the different powers of x are reduced mod y^2+1. If, in (2.6) we set $\alpha = 1$, we obtain

$$\frac{x+1}{x-1} = \frac{-y-1}{-y} = \frac{x^7}{x^6} = x ,$$

which gives an odd-powered residue. We shall now form the design where $\alpha = 1$. The first two blocks of the initial blocks are

$$\left[1_1,(-1)_1,x_2,-x_2\right],\ \left[x_1^2,-x_1^2,x_2^3,-x_2^3\right].$$

After substituting for x, the entire set of initial blocks is found to be

$$\left[(1)_1;(-1)_1;(-y+1)_3;(y-1)_3\right],\ \left[y_1;-y_1;(y+1)_2;(-y-1)_2\right];$$

$$\left[(1)_2;(-1)_2;(-y+1)_3;(y-1)_3\right],\ \left[y_2;-y_2;(y+1)_3;(-y-1)_3\right];$$

$$\left[(1)_3;(-1)_3;(-y+1)_1;(y-1)_1\right],\ \left[y_3;-y_3;(y+1)_1;(-y-1)_1\right];$$

$$(\infty;0_1;0_2;0_3).$$

In order to simplify the design, let the residues 0,1,-1,y,y+1, y-1,-y,-y+1,-y-1 be represented by 1,2,3,4,5,6,7,8,9 respectively. Writing the initial blocks first and adding the residues $x^0,x^1,\ldots,x^7$ to the initial blocks, we have the following design:

$(2_1,3_1,8_2,6_2),(4_1,7_1,5_2,9_2),(2_2,3_2,8_3,6_3),(4_2,7_2,5_3,9_3),(2_3,3_3,8_1,6_1),$
$(4_3,7_3,5_1,9_1),(\infty,1_1,1_2,1_3),(3_1,1_1,9_2,4_2),(5_1,8_1,6_2,7_2),(3_2,1_2,9_3,4_3),$
$(5_2,8_2,6_3,7_3),(3_3,1_3,9_1,4_1),(5_3,8_3,6_1,7_1),(\infty,2_1,2_2,2_3),(9_1,7_1,6_2,1_2),$
$(2_1,5_1,3_2,4_2),(9_2,7_2,6_3,1_3),(2_2,5_2,3_3,4_3),(9_3,7_3,6_1,1_1),(2_3,5_3,3_1,4_1),$
$(\infty,8_1,8_2,8_3),(5_1,6_1,2_2,9_2),(7_1,1_1,8_2,3_2),(5_2,6_2,2_3,9_3),(7_2,1_2,8_3,3_3),$
$(5_3,6_3,2_1,9_1),(7_3,1_3,8_1,3_1),(\infty,4_1,4_2,4_3),(6_1,4_1,3_2,7_2),(8_1,2_1,9_2,1_2),$
$(6_2,4_2,3_3,7_3),(8_2,2_2,9_3,1_3),(6_3,4_3,3_1,7_1),(8_3,2_3,9_1,1_1),(\infty,5_1,5_2,5_3),$
$(1_1,2_1,7_2,5_2),(6_1,9_1,4_2,8_2),(1_2,2_2,7_3,5_3),(6_2,9_2,4_3,8_3),(1_3,2_3,7_1,5_1),$
$(6_3,9_3,4_1,8_1),(\infty,3_1,3_2,3_3),(4_1,5_1,1_2,8_2),(9_1,3_1,7_2,2_2),(4_2,5_2,1_3,8_3),$
$(9_2,3_2,7_3,2_3),(4_3,5_3,1_1,8_1),(9_3,3_3,7_1,2_1),(\infty,6_1,6_2,6_3),(8_1,9_1,5_2,3_2),$
$(1_1,4_1,2_2,6_2),(8_2,9_2,5_3,3_3),(1_2,4_2,2_3,6_3),(8_3,9_3,5_1,3_1),(1_3,4_3,2_1,6_1),$
$(\infty,7_1,7_2,7_3),(7_1,8_1,4_2,2_2),(3_1,6_1,1_2,5_2),(7_2,8_2,4_3,2_3),(3_2,6_2,1_3,5_3),$
$(7_3,8_3,4_1,2_1),(3_3,6_3,1_1,5_1),(\infty,9_1,9_2,9_3).$

If $m=1$ in Theorem 2.3, the resulting design has the property that every variety occurs exactly t times in every position in the blocks. For the elements of the module represent the varieties and, no matter what element appears in a given position in a particular B_i, the addition of all elements of the module to this element leads to all the elements of the module in this position in the corresponding $B_{i\theta}$'s. This type of design is useful when the position in the block influences the yield.

Of particular interest are designs, which are termed symmetrical designs, formed by setting $v=b$, $r=k$. Once a symmetrical design has been constructed we can obtain three other designs from it. Denote the blocks of the symmetrical design by $B_1, B_2, \ldots, B_b$. The residual design is formed by deleting from the remaining blocks all the varieties that appeared in B_1. The derived design is formed by deleting from the symmetrical design all the varieties that do not appear in any one block, say B_1, and also deleting B_1.

Since there are k plots to a block in the symmetrical design and v varieties, there are v-k varieties in the residual design. Since one block has been deleted in forming both designs and since $v=b$, the number of blocks in both designs is v-1. When forming a residual design we delete all the varieties appearing in one block, so that the varieties remaining must occur the same number of times as in the symmetrical design. Similarly, the number of times a pair of varieties occurs in the same block in the symmetrical design remains unchanged in the residual design.

The number of varieties in a derived design is k since the design is formed by considering only those varieties which

appear in a given block and each block has k varieties. Each variety in the original design is replicated r times. Since we must delete one block containing all the varieties to be used, the number of times a variety is replicated in the derived design is k-1 since r = k. By deleting one block in which every pair of varieties under consideration appears, the number of times that each pair of varieties in the derived design appears together is λ -1 where λ is the number of times each pair of varieties occurred in the original design.

In order to show that these two designs are incomplete balanced block designs we need only to show that every block in a given design contains the same number of plots. We shall show below that the first block in a symmetrical design has exactly λ varieties in common with every other block. From this it follows that every block in the residual design contains $k-\lambda$ plots and every block in the derived design contains λ plots. Thus these designs are incomplete balanced block designs.

We now prove that every block in a symmetrical design has λ varieties in common with the first block. Let a_i be the number of varieties common to the first and the ith block, $i = 2,3,\ldots,b$. Then

$$\sum_{i=2}^{b} a_i = k(r-1), \tag{2.12}$$

since every one of the k varieties in the first block appears r-1 times in the remaining blocks. Also

$$\sum_{i=2}^{b} a_i \frac{(a_i-1)}{2} = (\lambda -1)\frac{k(k-1)}{2}. \tag{2.13}$$

For, in the set B_i, $i = 2,3,\ldots,b$, each pair of the k varieties in

B_1 occur in the same block λ-1 times. But there are $k\mathrm{C}2$ pairs of varieties. Hence there are $(\lambda-1)k\mathrm{C}2$ pairs of varieties in the blocks B_i, $i=2,3,\ldots,b$, which also appear in B_1. But since there are a_i varieties in B_1 common to B_i, there must be $a_i\mathrm{C}2 = a_i(a_i-1)/2$ pairs of varieties in B_1 which are also in B_i. Therefore $\sum_{i=2}^{b} a_i\mathrm{C}2$ represents the total number of pairs of varieties in $B_2,B_3,\ldots,B_b$ which are also in B_1. Hence (2.13) is valid.

Every variety v_i occurs in r blocks. In these r blocks there are r(k-1) varieties different from v_i. Since every pair of varieties occurs among the r blocks exactly λ times we have

$$r(k-1) = \lambda(v-1). \tag{2.14}$$

From (2.12) and (2.13) we have

$$\sum_i (a_i - \lambda)^2 = \sum a_i^2 - 2\lambda\sum a_i + (b-1)\lambda^2$$
$$= (\lambda-1)k(k-1) + k(r-1) - 2\lambda k(r-1) + (b-1)\lambda^2.$$

But since $k=r$, $b=v$, and from (2.14) we have

$$\sum_i (a_i - \lambda)^2 = k(k-1)\{\lambda - 1 + 1 - 2\lambda + \lambda\} = 0.$$

Hence $a_i = \lambda$, $i = 2,3,\ldots,b$.

Thus it follows that the derived and residual designs are incomplete balanced block designs having the parameter values $v=k'$, $b=v'-1$, $r=k'-1$, $k=\lambda'$, $\lambda=\lambda'-1$ and $v=v'-k'$, $b=v'-1$, $r=k'$, $k=k'-\lambda'$, $\lambda=\lambda'$ respectively where v',b',r',k',λ' are the parameter values of the original symmetrical design.

As an illustration demonstrating the processes of derivation and residuation consider the symmetrical design 25,25,9,9,3. This design was constructed by Bhattacharya (Bull. Calcutta Math. Soc. 36 (1945) pp. 91-96). The design is as follows:

1 2 5 6 11 12 17 20 23, 1 4 9 12 14 15 19 20 24,
1 2 9 10 15 17 16 21 25, 1 4 6 7 13 16 19 21 23,
1 2 7 8 13 14 17 22 24, 2 3 6 7 9 12 19 22 25,
3 4 7 8 9 10 17 20 23, 2 3 10 11 13 16 19 20 24,
3 4 11 12 13 14 17 21 25, 2 3 5 8 14 15 19 21 23,
1 3 5 7 10 12 18 21 24, 2 4 5 7 14 16 18 20 25,
1 3 9 11 14 16 18 22 23, 5 6 9 10 13 14 17 18 19,
1 3 6 8 13 15 18 20 25, 5 7 9 11 13 15 20 21 22,
2 4 6 8 9 11 18 21 24, 5 8 9 12 13 16 23 24 25,
2 4 10 12 13 15 18 22 23, 7 8 11 12 15 16 17 18 19,
3 4 5 6 15 16 17 22 24, 6 8 10 12 14 16 20 21 22,
1 4 5 8 10 11 19 22 25, 6 7 10 11 14 15 23 24 25,
17 18 19 20 21 22 23 24 25.

From the above symmetrical design form the residual pattern by deleting all varieties in the last block. The values of the parameters from previous work are seen to be $v = 16$, $b = 24$, $r = 9$, $k = 6$, $\lambda = 3$. The design is given by the following:

1 2 5 6 11 12, 1 2 7 8 13 14, 3 4 11 12 13 14,
1 2 9 10 15 16, 3 4 7 8 9 10, 3 4 5 6 15 16,
1 4 5 8 10 11, 1 3 5 7 10 12, 5 6 9 10 13 14,
1 4 9 12 14 15, 1 3 9 11 14 16, 5 7 9 11 13 15,
1 4 6 7 13 16, 1 3 6 8 13 15, 5 8 9 12 13 16,
2 3 6 7 9 12, 2 4 6 8 9 11, 7 8 11 12 15 16,
2 3 10 11 13 16, 2 4 10 12 13 15, 6 8 10 12 14 16,
2 3 5 8 14 15, 2 4 5 7 14 16, 6 7 10 11 14 15.

Next we form the derived design by considering the varieties

which appear in the first block only of the symmetrical design. The parameters for this derived design v,b,r,k,λ, have the values 9,24,8,3,2 respectively. The design is given by the following:

1 2 17,	1 11 23,	2 11 20,	6 11 23,
1 2 17,	1 12 20,	2 12 23,	6 12 20,
1 5 11,	2 5 20,	5 6 17,	11 12 17,
1 5 12,	2 5 23,	5 6 17,	11 12 17,
1 6 20,	2 6 11,	5 11 20,	17 20 23,
1 6 23,	2 6 12,	5 12 23,	17 20 23.

Notice the four pairs of identical blocks formed in this design.

Finally we see that from every incomplete balanced block design $B_1,\ldots,B_b$ another incomplete balanced block design $B_1',\ldots,B_b'$ can be formed by putting into each B_i' all the varieties not in the corresponding B_i. The design formed is called the complementary design.

Since there are k varieties contained in each of the B_i's, there are v-k varieties in each corresponding B_i'. Since no variety appears more than once in a block, $r \leq b$. In practice $r < b$, since $r = b$ and the relation $bk = rv$ imply that $k = v$. In this case every variety appears in every block and the design is not a useful one. Since $r < b$, some B_i does not contain any given variety and hence this variety is contained in B_i'. Thus all v varieties appear in the complementary design. Every variety appears in the B_i's exactly r times. Since every variety appears in a B_i' once for each time that it doesn't appear in the corresponding B_i, then each variety appears in the complementary design exactly b-r times.

Consider next a pair of varieties in the B_i's. A given pair of varieties appears in λ blocks. Each variety of the pair appears in r blocks. Hence the number of blocks in which one or more of the varieties appears is $2r-\lambda$. The number of blocks in which neither appear is $b-2r+\lambda$ and this is the number of blocks in which the pair of varieties will appear in the complementary design. Hence the parameter values for the complementary design are v, b, $b-r, v-k, b-2r+\lambda$.

At the present time there are a great many designs available but as yet necessary and sufficient conditions for the existence of an incomplete balanced block design with given parameters are not known. The relations $bk = rv$ and $r(k-1) = \lambda(v-1)$ are necessary conditions only. Another necessary condition, which we shall now prove is that $b \geq v$ if $v > k$. Since $bk = rv$, $b \geq v$ if and only if $r \geq k$. From (2.13) and (2.14)

$$\sum_{i=2}^{b} a_i^2 = (\lambda-1)k(k-1) + \sum_{i=2}^{b} a_i$$
$$= k\left[(\lambda-1)k + r - \lambda\right].$$

Also from (2.13) the mean of the a_i's is $\bar{a}_i = k(r-1)/(b-1)$. Therefore

$$\sum_i (a_i - \bar{a}_i)^2 = \sum_i \left[a_i^2 - 2a_i\bar{a}_i + \bar{a}_i^2\right]$$
$$= \sum_i a_i^2 - (b-1)\bar{a}_i^2 \geq 0.$$

Thus

$$\sum_i a_i^2 \geq (b-1)\bar{a}_i^2 = k^2(r-1)^2/(b-1).$$

Hence

(2.15) $$(\lambda-1)k + r - \lambda \geq k(r-1)^2/(b-1).$$

Since $r(k-1) = \lambda(v-1)$, we have $rk - r = \lambda v - \lambda$, i.e.,

(2.16) $$r-\lambda = rk-\lambda v.$$

Substituting for $r-\lambda$ in (2.15), we have

$$(\lambda -1)k + rk-\lambda v \geq k(r-1)^2/(b-1),$$

which can be written as

$$k(r-1)-k(r-1)^2/(b-1) \geq \lambda(v-k),$$

or

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

From $bk = rv$ we have

(2.18) $$\frac{b-r}{v-k} = \frac{r}{k}.$$

Since $v > k$, dividing (2.17) by $v-k$ and using (2.17) we have

$$r(r-1) \geq \lambda(b-1).$$

Subtracting this from $r(k-1) = \lambda(v-1)$ we have

$$r(r-k) \geq \lambda(b-v).$$

But again from $bk = rv$, $(b-v)/v = (r-k)/k$. Therefore

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

and

$$rk(r-k) - \lambda v(r-k) \geq 0$$

i.e.,

$$(r-k)(rk-\lambda v) \geq 0.$$

But $kr-\lambda v = r-\lambda$ by (2.16). Since $v > k$ and $r(k-1) = \lambda(v-1)$, it follows that $r-\lambda > 0$. Hence $r \geq k$ and $b \geq v$.

CHAPTER III

THE ANALYSIS OF LATIN SQUARES

In this chapter we shall consider a test which will be used in testing linear hypotheses. We consider first a set of N random variables $y_1, y_2, \ldots, y_N$ and put $E(y_\alpha) = \mu_\alpha$. We now make the following assumptions.

(1) The y_α are normally and independently distributed and their variances, σ^2, are equal.

(2) The μ_α are linear functions of p parameters $\beta_1, \beta_2, \ldots, \beta_p$, where $p < N$; i.e.,

$$\mu_\alpha = \sum_{i=1}^{p} g_{i\alpha}\beta_i, \qquad \alpha = 1, \ldots, N, \tag{3.1}$$

and the rank of the matrix $(g_{i\alpha})$ is equal to p, where α denotes the row number.

By eliminating the β_i from (3.1) we see[1] that assumption (2) reduces to the equivalent assumption that the μ_α satisfy N-p restrictions of the form

$$\sum_{\alpha} \lambda_{k\alpha}\mu_\alpha = 0, \quad \text{where } k = 1, \ldots, N-p, \tag{3.2}$$

and the rank of the matrix $(\lambda_{k\alpha}) = N-p$.

The hypothesis we wish to test is that the β_j satisfy s independent linear restrictions, i.e.,

$$\sum_{j=1}^{p} k_{ij}\beta_j = 0, \quad i = 1, \ldots, s, \quad s < p. \tag{3.3}$$

By eliminating the β_j from (3.1) and (3.3), the hypothesis (3.3)

---

[1] Attridge, R.F., Linear Regression and Multiple Classification Designs. 1952, p. 113.

may be written[1] in the form

$$\sum_{\alpha=1}^{N} \rho_{k\alpha}\mu_\alpha = 0, \quad k=1,\ldots,s. \tag{3.4}$$

It can be shown[2] that equations (3.2) and (3.4) consist of N-p+s linearly independent equations. We can now introduce the following theorems.

Theorem 3.1: Let $y_1, y_2, \ldots, y_N$ be normally and independently distributed variables with the same variance and means $\mu_1, \mu_2, \ldots, \mu_N$ respectively. Assume that the μ_α satisfy the following independent relations,

$$\sum_{\alpha=1}^{N} \lambda_{i\alpha}\mu_\alpha = 0, \quad i=1,\ldots,N-p \tag{3.5}$$

In order to test the hypothesis that the μ_α satisfy the relations

$$\sum_{\alpha=1}^{N} \rho_{i\alpha}\mu_\alpha \quad , \quad i=1,\ldots,s; \quad s \leq p, \tag{3.6}$$

which are independent of the relations (3.5) and of each other, we form the ratio

$$F = \frac{N-p}{s} \cdot \frac{Q_r - Q_a}{Q_a} \quad , \tag{3.7}$$

where Q_a is the minimum with respect to μ_α of $\sum_{\alpha=1}^{N}(y_\alpha - \mu_\alpha)^2$ under the restrictions (3.5) and (3.6). We reject the hypothesis (3.6) if $F \geq F_o$ where $P(F \geq F_o \mid (3.5) \text{ and } (3.6)) = \alpha$ and α is a fixed constant. Then

(1) the test described above is equivalent to the likelihood ratio test for the hypothesis (3.6);

(2) the ratio (3.7) has the F distribution with s and N-p degrees of freedom respectively.

---

[1] Attridge, p. 114.

[2] Mann, Analysis and Design of Experiments. Dover 1949. New York, P. 24.

It should be observed that the relations (3.1) and (3.3) are equivalent to equations (3.5) and (3.6) respectively, viz.,

$$\mu_\alpha = \sum_{i=1}^{p} g_{i\alpha}\beta_i , \qquad \alpha = 1,\ldots,N,$$

$$\sum_{j=1}^{p} k_{ij}\beta_j = 0 , \qquad i = 1,\ldots,s.$$

If $b_1,\ldots b_p$ are the values of $\beta_1,\ldots,\beta_p$ which minimize $\sum_{\alpha=1}^{N}(y_\alpha-\mu_\alpha)^2$ under a set of linear restrictions

$$Y_\alpha = \sum_{i=1}^{p} g_{i\alpha} b_i$$

is called the regression value of y_α.

Theorem 3.2: Let $H_1,\ldots,H_s$ be a sequence of hypotheses on the means of the variables y with $E(y_\alpha)=\mu_\alpha$ of the form

$$H_1: \mu_\alpha = \sum_{i=1}^{p} g_{i\alpha}\beta_i,$$

$$H_2: H_1 \text{ and } \sum_{j=1}^{p} a_{kj}\beta_j = 0, \qquad k = 1,\ldots,s,$$

$$\cdots$$

$$H_t: H_{t-1} \text{ and } \sum_{j=1}^{p} a_{kj}\beta_j = 0, \qquad k = s_{t-2}+1,\ldots,s_{t-1} \text{ where } s_{t-1} < p,$$

such that the linear restrictions imposed by H_s are linearly independent of each other. Let $Y_\alpha^{(t)}$ be the regression value of y_α obtained under the hypothesis H_t, then

$$\sum_\alpha y_\alpha^2 = \sum_\alpha (y_\alpha - Y_\alpha^{(1)})^2 + \sum_\alpha (Y_\alpha^{(1)} - Y_\alpha^{(2)})^2 + \ldots + \sum_\alpha (Y_\alpha^{(s-1)} - Y_\alpha^{(s)})^2 + \sum_\alpha (Y_\alpha^{(s)})^2.$$

Proof: See Attridge page 145.

Theorem 3.3: Let Q_a be the minimum of the quadratic form $Q = \sum_\alpha (y_\alpha - E(y_\alpha))^2$ under the assumption

$$E(y_\alpha) = \sum_{i=1}^{s} \beta_i g_{i\alpha} + \sum_{d=s+1}^{p} \beta_d g_{d\alpha} , \qquad \alpha = 1,\ldots,N, \tag{3.7}$$

and Q_r its minimum under the additional restrictions $\beta_i = 0, i = 1,\ldots,s.$

Let b_i, $(i = 1,\ldots,s)$, b_d $(d = s+1,\ldots,p)$ be the least square estimates of $\beta_1, \beta_2,\ldots,\beta_p$ under the assumption (3.7) and put

$$\left(\frac{\sigma_{b_i b_j}}{\sigma^2}\right)^{-1} = (c_{ij}), \quad i,j = 1,\ldots,s.$$

Then

$$Q_r - Q_a = \sum_{i=1}^{s}\sum_{j=1}^{s} c_{ij} b_i b_j.$$

Proof: See Attridge, page 151.

The regression coefficient β_p is called the general mean.

Corollary 3.3: Let the hypothesis in Theorem 3.3 be

$$\beta_i^* = \sum_{t=1}^{p} \ell_{it}\beta_t = 0 \quad , \qquad i = 1,\ldots,s \leq p$$

where the rank of (ℓ_{it}) is s. Put

$$\sum_{t=1}^{p} \ell_{it} b_t = b_i^* \text{ and } \left(\frac{\sigma_{b_i^* b_j^*}}{\sigma^2}\right)^{-1} = (c_{ij}),$$

then

$$Q_r - Q_a = \sum_{i=1}^{s}\sum_{j=1}^{s} c_{ij} b_i b_j .$$

The most important special case of the above theorem and its corollary is the case where $s = 1$ and

$$Q_r - Q_a = \frac{b_1^2 \sigma^2}{\sigma_{b_1}^2}$$

Theorem 3.4: Let

$$E(y_\alpha) = \mu_\alpha = \sum_{i=1}^{p} g_{i\alpha}\beta_i .$$

Assume that

(1) $g_{p\alpha} = 1$ for all α and hence β_p is the general mean;

(2) $g_{i\alpha}$ is either 0 or 1, $i = 1,\ldots,s$, $s < p$;

(3) $\sum_{\alpha=1}^{N} g_{i\alpha} g_{j\alpha} = 0$ if $i \neq j$, $i,j \leq s$;

(4) $\sum_{i=1}^{s} g_{i\alpha}^2 = 1$, $\alpha = 1,\ldots,N$.

In view of assumption (2), assumption (4) implies that all the first s $g_{i\alpha}$ for any one row are zero except one and its value is 1.

If

$$Q = \sum_{\alpha=1}^{N} (y_\alpha - \sum_{i=1}^{p} g_{i\alpha} \beta_i)^2$$

is minimized with respect to $\beta_1, \ldots, \beta_p$ and

$$\sum_{i=1}^{s} t_i \beta_i = 0, \quad \sum_{i=1}^{s} t_i \neq 0,$$

is the only restriction on $\beta_1, \ldots, \beta_s, \beta_p$, and if λ_1 is the Lagrange multiplier associated with $\sum_{i=1}^{s} t_i \beta_i = 0$, then $\lambda_1 = 0$.

Proof: See Attridge page 161.

We shall now use this theory in the development of the analysis of a single m x m Latin square. We shall assume that the mean yield $E(y_{ijk})$ of the kth variety on the plot in the ith row and jth column of the Latin square is given by

(3.8) $$\sum (y_{ijk}) = \mu_i + \nu_j + \rho_k + \rho ,$$

(3.9) $$\sum_i \mu_i = \sum_j \nu_j = \sum_k \rho_k = 0 .$$

The quantities μ_i, ν_j, ρ_k, are called row, column, and varietal effects respectively where every variety appears once in every row and column. The first hypothesis we wish to test is

$$H: \mu_i = 0, \ i = 1, \ldots, m.$$

First we must compute Q_a, which is the minimum of Q, where

(3.10) $$Q = \sum_{i=1}^{m} \sum_{j=1}^{m} (y_{ijk} - \mu_i - \nu_j - \rho_k - \rho)^2$$

subject to conditions (3.9). Now (3.8) may be written as

(3.11) $$E(y_{ijk}) = \sum_{i'=1}^{m} \delta_{ii'} \mu_{i'} + \sum_{j'=1}^{m} \delta_{jj'} \nu_{j'} + \sum_{k'=1}^{m} \delta_{kk'} \rho_{k'} + \rho$$

where $\delta_{\alpha\beta}$ is the Kronecker delta. Now apply Theorem 3.4,

where (3. 11) is equivalent to $\sum_{i=1}^{\rho} g_{i\alpha}\beta_i$, and also where $s=m$, $p=3m+1$ and $\alpha=1,\ldots,m^2$. We see that (3.11) has the following properties regarding the matrix of coefficients $(g_{i\alpha})$:

(1) every element in the last column is 1 , i.e., $g_{p\alpha}=1$ for all α ;

(2) the first s elements in each ~~column~~ row are either zero or one;

(3) the first s columns are orthogonal , i.e., $\sum_{\alpha=1}^{N} g_{i\alpha}g_{j\alpha} = 0$ for $i\neq j$, $i,j\leq s$;

(4) exactly one of the first s elements in each row has the value one and the rest are zero.

Hence we see that (3.11) satisfies the four postulates of Theorem 3.4. Hence, in finding Q_a, we may ignore condition (3.9). Thus, to find Q_a we minimize Q in (3.10). We have

$$(3.12)\qquad -\frac{1}{2}\frac{\partial Q}{\partial \mu_i} = \sum_{j=1}^{m}(y_{ijk}-\mu_i-\nu_j-\rho_k-\rho) = 0.$$

For i fixed, as j goes from 1 to m, k goes from 1 to m. Hence (3.12) reduces to

$$my_{i..}-m\mu_i-0-\sum_{k=1}^{m}\rho_k-m\rho = 0,$$

which may be further reduced to

$$(3.13)\qquad y_{i..}-\mu_i-\rho = 0,$$

where $y_{i..}$ is the mean of the observations in the ith row. Similarly $\partial Q/\partial \nu_j = 0$ gives the following equation,

$$(3.14)\qquad y_{.j.}-\nu_j-\rho = 0$$

where $y_{.j.}$ is the mean of the observations in the jth column. Also

$$(3.16)\qquad -\frac{1}{2}\frac{\partial Q}{\partial \rho_k} = \sum_{ij}(y_{ijk}-\mu_i-\nu_j-\rho_k-\rho) = 0$$

where $\sum_{ij}$ means the sum over all values of i,j, which give our

given value of k. Now (3.16) may be reduced to

(3.17) $$y_{..k} - \rho_k - \rho = 0,$$

where $y_{..k}$ is the mean of all the observations on the kth variety. Finally

$$-\frac{1}{2}\frac{\partial Q}{\partial \rho} = \sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk} - \mu_i - \nu_j - \rho_k - \rho) = 0.$$

This can be reduced to $y - \rho = 0$, where y is the grand mean.

Summing up, we see that the estimates of μ_i, ν_j, ρ_k, and ρ which minimize Q in (3.10) denoted by $\hat{\mu}_i$, $\hat{\nu}_j$, $\hat{\rho}_k$, and $\hat{\rho}$, are

(3.19) $$\begin{aligned} \hat{\mu}_i &= y_{i..} - y, \\ \hat{\nu}_j &= y_{.j.} - y, \\ \hat{\rho}_k &= y_{..k} - y, \\ \hat{\rho} &= y. \end{aligned}$$

Then Q_a is given by the following expression,

$$Q_a = \sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk} - y_{i..} - y_{.j.} - y_{..k} + 2y)^2.$$

Now apply Theorem 3.2 with the following chain of hypothesis:

(3.20) $$\begin{aligned} &H_1: E(y_{ijk}) = \mu_i + \nu_j + \rho_k + \rho, \ \sum_i \mu_i = \sum_j \nu_j = \sum_k \rho_k = 0 \\ &H_2: H_1 \text{ and } \mu_i = 0, \ (i = 1,\ldots,m), \\ &H_3: H_2 \text{ and } \nu_j = 0, \ (j = 1,\ldots,m), \\ &H_4: H_3 \text{ and } \rho_k = 0, \ (k = 1,\ldots,m). \end{aligned}$$

Now from H_1 we have that

(3.21) $$Y^{(1)}_{ijk} = y_{i..} + y_{.j.} + y_{..k} - 2y.$$

Under H_2 we minimize

$$Q = \sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk} - \nu_j - \rho_k - \rho)^2.$$

Hence we have

$$-\frac{1}{2}\frac{\partial Q}{\partial \nu_j} = \sum_{i=1}^{m}(y_{ijk} - \nu_j - \rho_k - \rho) = 0$$

which reduces to

(3.22) $$y_{.j.} - \nu_j - \rho = 0.$$

Similarly $\partial Q/\partial \rho_k = 0$ reduces to

(3.23) $$y_{..k} - \rho_k - \rho = 0,$$

and $\partial Q/\partial \rho = 0$ reduces to

(3.24) $$y - \rho = 0.$$

Thus from H_2 and (3.22), (3.23), and (3.24) we have that

$$Y^{(2)}_{ijk} = y_{.j.} + y_{..k} - y.$$

From H_3 and (3.23) and (3.24) we have that

$$Y^{(3)}_{ijk} = y_{..k}.$$

Under H_4 and from (3.24) we see that

$$Y^{(4)}_{ijk} = y.$$

Thus from Theorem 3.2 we have that

$$\sum_{i=1}^{m}\sum_{j=1}^{m} y^2_{ijk} = Q_a + \sum_i\sum_j (y_{i..} - y)^2 + \sum_i\sum_j (y_{.j.} - y)^2 + \sum_i\sum_j (y_{..k} - y)^2 + \sum_i\sum_j y^2.$$

This may be written as

(3.25) $$\sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk} - y)^2 = Q_a + m\sum_{i=1}^{m}(y_{i..} - y)^2 + m\sum_{j=1}^{m}(y_{.j.} - y)^2 + m\sum_{k=1}^{m}(y_{..k} - y)^2$$

Equation (3.25) is very convenient for computing Q_a as all the other sums involved can be computed readily for a given problem.

The hypothesis we wish to test now is

$$H: \mu_1 = \mu_2 = \cdots = \mu_m = 0$$

First we must compute Q_r where Q_r is the minimum of Q in (3.10) under the original assumptions of (3.9) and our hypothesis. Hence the expression to be minimized under these conditions becomes

(3.26) $$Q = \sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk} - \nu_j - \rho_k - \rho)^2.$$

As before $s = m$. Since under the present hypothesis we can delete the first m parameters, we have that $p = 2m + 1$. As in the former case it can be verified that the conditions of Theorem 3.4 hold. Hence we may ignore the conditions

$$\sum_j \nu_j = \sum_k \rho_k = 0 .$$

Minimizing Q in (3.26) we have

$$-\frac{1}{2}\frac{\partial Q}{\partial \nu_j} = \sum_{i=1}^{m} (y_{ijk} - \nu_j - \rho_k - \rho) = 0$$

which reduces to

$$y_{.j.} - \nu_j - \rho = 0. \tag{3.27}$$

Similarly $\partial Q/\partial \rho_k = 0$ reduces to

$$y_{..k} - \rho_k - \rho = 0, \tag{3.28}$$

and $\partial Q/\partial \rho = 0$ reduces to

$$y - \rho = 0. \tag{3.29}$$

Hence our estimates of ν_j, ρ_k, and ρ, which minimize Q in (3.26) are given by $\hat{\nu}_j$, $\hat{\rho}_k$, and $\hat{\rho}$. They are

$$\begin{aligned} \hat{\nu}_j &= y_{.j.} - y, \\ \hat{\rho}_k &= y_{..k} - y, \\ \hat{\rho} &= y. \end{aligned} \tag{3.30}$$

It should be observed that the estimates of ν_j, ρ_k, ρ, in (3.30) are exactly the same set of values which were used in determining Q_a.

We shall now set up the chain of hypotheses H_1', H_2', H_3', where H_1' is H_2, H_2' is H_3, and H_3' is H_4 where H_2, H_3, H_4 are given by (3.20). Now applying Theorem 3.2 and using the above hypotheses we have that $Y_{ijk}^{(1)'} = Y_{ijk}^{(2)}$, $Y_{ijk}^{(2)'} = Y_{ijk}^{(3)}$, $Y_{ijk}^{(3)'} = Y_{ijk}^{(4)}$, where $Y_{ijk}^{(s)}$, $s = 1, 2, 3$, are the regression values in determining Q_a. We have

$$\sum_{i=1}^{m}\sum_{j=1}^{m} y_{ijk}^2 = Q_r + \sum_i \sum_j (y_{.j.} - y)^2 + \sum_i \sum_j (y_{..k} - y)^2 + \sum_i \sum_j y^2 .$$

This may be written

$$\sum_i \sum_j (y_{ijk}-y)^2 = Q_r + m\sum_j (y_{.j.}-y)^2 + m\sum_k (y_{..k}-y)^2. \tag{3.31}$$

Solving for Q_r in (3.31) and using the value of Q_a in (3.25) we have

$$Q_r - Q_a = m \sum_{i=1}^{m} (y_{i..}-y)^2. \tag{3.32}$$

In Theorem 3.1 our original assumptions were

$$\mu_\alpha = \sum_{i=1}^{p} g_{i\alpha}\beta_i , \qquad \alpha = 1,\ldots,N,$$

where the rank of $(g_{i\alpha})$ is p. In our case, in addition to the conditions of the above form, we have three additional conditions, viz.,

$$\sum_i \mu_i = \sum_j \nu_j = \sum_k \rho_k = 0, \qquad i,j,k = 1,\ldots,m. \tag{3.33}$$

By eliminating μ_m, ν_m, ρ_m from (3.11) where μ_m, ν_m, ρ_m are determined from (3.33) we have reduced our problem to a type which can be solved by using Theorem 3.1.

From (3.33) we have that

$$\mu_m = -\sum_{i=1}^{m-1} \mu_i , \quad \nu_m = -\sum_{j=1}^{m-1} \nu_j , \quad \rho_m = \sum_{k=1}^{m-1} \rho_k . \tag{3.34}$$

Relabel the parameters $\mu_1,\ldots,\mu_{m-1}, \nu_1,\ldots,\nu_{m-1}, \rho_1,\ldots,\rho_{m-1}, \rho$ as $\beta_1,\ldots,\beta_{m-1}, \beta_m,\ldots,\beta_{2m-2}, \beta_{2m-1},\ldots,\beta_{3m-3}, \beta_{3m-2}$, respectively. We may write (3.11) in the following form

$$E(y_{ijk}) = \sum_{p=1}^{3m-2} g_{pij}\beta_p, \quad i,j = 1,\ldots,m, \tag{3.35}$$

where the column number of the matrix of coefficients (g_{pij}) is given by p and the row number by ij.

Our problem now reduces to finding the rank of $G = (g_{pij})$. The rank of G is the rank of its Gram matrix[1] $S = G'G$ where G' is

---

[1] Schwerdtfeger. Introduction to Linear Algebra and The Theory of Matrices. Groningen, Holland: P. Noordhoff N.V., 1950, p. 142.

the transpose of G. From (3.11) and (3.34) we have

$$(3.36)\qquad \sum_{p=1}^{3m-2} g_{p,ij}\,\beta_p = \sum_{i'=1}^{m-1}(\delta_{ii'}-\delta_{im})\mu_{i'} + \sum_{j'=1}^{m-1}(\delta_{jj'}-\delta_{jm})\nu_{j'} + \sum_{k'=1}^{m-1}(\delta_{kk'}-\delta_{km})\rho_{k'} + \rho$$

From (3.36) we have the following relations,

$$(3.37)\qquad \begin{aligned} g_{p,ij} &= \delta_{ip} - \delta_{im}, \quad p = 1,\ldots,m-1,\\ g_{p,ij} &= \delta_{j,p-m+1} - \delta_{jm}, \quad p = m,\ldots,2m-2,\\ g_{p,ij} &= \delta_{k,p-2m-2} - \delta_{km}, \quad p = 2m-1,\ldots,2m-3,\\ g_{3m-2,ij} &= 1. \end{aligned}$$

Let $S = (a_{pq})$, where S is a square matrix of order 3m-2. The general element of S, viz., a_{pq}, is the sum of the product of the elements in the pth row of G' and the qth column of G. Since the rows of G' are the columns of G, a_{pq} is thus the sum of the products of the elements in the pth column and the qth column of G. Hence we see that $a_{pq} = a_{qp}$.

Consider the submatrix (a_{pq}), $p,q = 1,\ldots,m-1$, where p denotes the row number. From (3.37) the diagonal elements a_{pp} are given by

$$\begin{aligned} a_{pp} &= \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{ip}-\delta_{im})^2\\ &= \sum_{j}(2) = 2m. \end{aligned}$$

The non-diagonal elements are given by

$$\begin{aligned} a_{pq} &= \sum_{i}\sum_{j}(\delta_{ip}-\delta_{im})(\delta_{iq}-\delta_{im}), \quad p,q = 1,\ldots,m, \quad p \neq q,\\ &= \sum_{j}(1) = m. \end{aligned}$$

Hence the submatrix in the upper left hand corner of S would be

$$(3.38)\qquad A_1 = \begin{pmatrix} 2m & m & \cdots & m\\ m & 2m & & \cdot\\ \cdot & \cdot & & \cdot\\ \cdot & & \cdot & \cdot\\ m & \cdots & & 2m \end{pmatrix}$$

where A_1 is a square matrix of order m-1.

Next consider the submatrix $A_2 = (a_{pq})$, $p = 1,\ldots,m-1; q = m,\ldots,2m-2$. From (3.37) the general term is given by

$$a_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{ip} - \delta_{im})(\delta_{j,q-m+1} - \delta_{jm})$$

$$= \sum_{j}(\delta_{j,q-m+1} - \delta_{jm}) \cdot \sum_{i}(\delta_{ip} - \delta_{im}) = 0$$

since the last sum is zero. We thus have that A_2 is a square matrix all of whose elements are zero. Since $a_{pq} = a_{qp}$ we have that A_4, where $A_4 = (a_{pq})$, $p = m,\ldots,2m-2$, $q = 1,\ldots,m-1$, is equal to A_2.

We compute next $A_3 = (a_{pq})$, $p = 1,\ldots,m-1$, $q = 2m-1,\ldots,3m-3$. From (3.37) we have

$$a_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{ip} - \delta_{im})(\delta_{k,q-2m+2} - \delta_{km})$$

$$= \sum_{i=1}^{m}\left[(\delta_{ip} - \delta_{im}) \cdot \sum_{j=1}^{m}(\delta_{k,q-2m+2} - \delta_{km})\right]$$

$$\sum_{i=1}^{m}\left[(\delta_{ip} - \delta_{im}) \cdot \sum_{k=1}^{m}(\delta_{k,q-2m+2} - \delta_{km})\right]$$

$$= 0$$

since the last sum is zero. This follows from the fact that $1 \leq q-2m+2 \leq m-1$. Hence A_3 is an (m-1)st zero square matrix. By the same argument as presented before we have that $A_7 = A_3$ where $A_7 = (a_{pq})$, $p = 2m-1,\ldots,3m-2$, $q = 1,\ldots,m-1$.

We shall determine next $A_6 = (a_{pq})$, $p = m,\ldots,2m-2$, $q = 2m-1,\ldots,3m-3$. From (3.37) we have

$$a_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{j,p-m+1} - \delta_{jm})(\delta_{k,q-2m+2} - \delta_{km})$$

$$= \sum_{j=1}^{m}\left[(\delta_{j,p-m+1} - \delta_{jm}) \cdot \sum_{i=1}^{m}(\delta_{k,q-2m+2} - \delta_{km})\right]$$

$$= \sum_{j=1}^{m}\left[(\delta_{j,p-m+1} - \delta_{jm}) \sum_{k=1}^{m}(\delta_{k,q-2m+2} - \delta_{km})\right]$$

$$= 0 ,$$

since the last sum is zero, which follows since $1 \leq q-2m+2 \leq m-1$. Hence A_6 is the $(m-1)$st square matrix all of whose elements are zero. By previous reasoning we have $A_8 = A_6$ where $A_8 = (a_{pq})$, $p = 2m-1,\ldots,3m-3; q = m,\ldots,2m-2$.

We now compute the diagonal submatrix $A_5 = (a_{pq})$, $p = m,\ldots,2m-1; q = m,\ldots,2m-1$. From (3.37) the diagonal elements are given by

$$a_{pp} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{j,p-m+1} - \delta_{jm})^2$$

$$= \sum_{i=1}^{m}(2) = 2m,$$

where $1 \leq p-m+1 \leq m-1$. The non-diagonal elements are given by

$$a_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{j,p-m+1} - \delta_{jm})(\delta_{j,q-m+1} - \delta_{jm}),$$

where $p,q = m,\ldots,2m-1$, and $p \neq q$. This reduces to

$$a_{pq} = \sum_{i=1}^{m}(1) = m.$$

Hence we have that A_5 is the $m-1$ square matrix given by (3.38).

The remaining matrix to be computed is the diagonal submatrix $A_9 = (a_{pq})$, $p,q = 2m-1,\ldots,3m-3$. From (3.37) the diagonal elements are given by

$$a_{pp} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{k,p-2m+2} - \delta_{km})^2$$

$$= \sum_{i=1}^{m}\left[\sum_{j=1}^{m}(\delta_{k,p-2m+2} - \delta_{km})^2\right]$$

$$= \sum_{i=1}^{m}\left[\sum_{k=1}^{m}(\delta_{k,p-2m+2} - \delta_{km})^2\right]$$

$$= \sum_{i=1}^{m}(2) = 2m$$

since $1 \leq p-2m+2 \leq m-1$. The non- diagonal elements are given by

$$a_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{k,p-2m+2} - \delta_{km})(\delta_{k,q-2m+2} - \delta_{km}),\ p \neq q,$$

$$= \sum_{i=1}^{m}\left[\sum_{j=1}^{m}(\delta_{k,p-2m+2} - \delta_{km})(\delta_{k,q-2m+2} - \delta_{km})\right]$$

$$= \sum_{i=1}^{m}\left[\sum_{k=1}^{m}(\delta_{k,p-2m+2} - \delta_{km})(\delta_{k,q-2m+2} - \delta_{km})\right]$$

$$= \sum_{i=1}^{m}(-1)(-1) = m.$$

Hence we see that $A_9 = A_1 = A_4$.

The only remaining elements to be determined in the matrix S are the elements in the last row and last column. Since S is a symmetric matrix, in essence we have only to compute the elements in the last column, i.e., we have to compute $a_{p,3m-2}$, $1 \leq p \leq 3m-2$. Since $g_{3m-2,ij} = 1$, we have that all the elements in the last column of G are equal to one. From G'G we see that

$$a_{3m-2,3m-2} = \sum_{i=1}^{m}\sum_{j=1}^{m}(1) = m^2.$$

Also

$$a_{p,3m-2} = \sum_{i=1}^{m}\sum_{j=1}^{m} g_{pij} = 0,\ p = 1,\ldots,3m-3.$$

Thus we see that all the elements in the last column of S are zero except the last one which has the value m^2. Hence we may write S as

$$S = \begin{pmatrix} A_1 & 0_{m-1} & 0_{m-1} & 0 \\ 0_{m-1} & A_1 & 0_{m-1} & 0 \\ 0_{m-1} & 0_{m-1} & A_1 & 0 \\ 0 & 0 & 0 & m^2 \end{pmatrix}$$

where A_1 is the (m-1)-rowed square matrix given by (3.38), and 0_{m-1} is the (m-1)-rowed zero square matrix. From Laplace's development by columns[1] the value of the determinant of S is equal to

---

[1] Dickson, First Course in The Theory of Equations. Wiley, New York, 1922: p. 122.

$m^2|A_1|^3$ where $|A_1|$ is the determinant of A_1.

Consider the kxk determinant

$$\begin{vmatrix} b & a & \dots & a \\ a & b & a & \dots a \\ \cdot & \cdot & & \cdot \\ \cdot & & \cdot & \cdot \\ \cdot & & \cdot & \cdot \\ a & \dots & & b \end{vmatrix} = \begin{vmatrix} b & a & a & \dots & a \\ a-b & b-a & 0 & \dots & a \\ a-b & 0 & b-a & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ a-b & 0 & 0 & \dots & b-a \end{vmatrix}$$

$$= \begin{vmatrix} b+(k-1)a & a & a & \dots & a \\ 0 & b-a & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot & \cdot \\ \cdot & \cdot & & & \cdot \\ 0 & 0 & \dots & 0 & b-a \end{vmatrix} = \Big[b+(k-1)a\Big](b-a)^{k-1}.$$

Thus, for $|A|$, $b=2m$, $a=m$, $k=m-1$, we have

$$|A| = m^{m-2}\Big[(m-2)m+2m\Big] = m^m.$$

Hence it follows that $|S| \neq 0$. Since S is a square matrix of side 3m-2 its rank must be 3m-2. Hence G is also of rank 3m-2.

By Theorem 3.1, the rank of Q_a, which is also called its number of degrees of freedom, is

$$m^2 - (3m-2) = (m-1)(m-2).$$

It remains to determine the rank of

$$Q_r - Q_a = m\sum_{i=1}^{m}(y_{i..}-y)^2.$$

To do so we need the following two theorems

Theorem 3.5: The rank of a sum of quadratic forms is equal to or less than the sum of the ranks of the forms.

Proof: See Mann pp. 9.10.

Theorem 3.6: If a quadratic form $Q = \sum_{i=1}^{p} L_i^2$ where

$$L_i = \sum_{j=1}^{n} a_{ij}x_j \ , \quad i=1,\dots,p,$$

and the L_i are related by h linearly independent linear homogeneous relations,

$$r(Q) \leqq p-h,$$

where r(Q) denotes the rank of Q.

Proof: See Attridge p. 30.

The above theorem may be applied to Q_r-Q_a since the presence of the constant m does not affect the rank of the quadratic form. We note that $y_{i..}-y$ is a linear form in the y_{ijk}'s. Also

$$\sum_{i=1}^{m}(y_{i..}-y) = my-my = 0,$$

so that we have one linear homogeneous relation among the $y_{i..}-y$. Hence the rank of $m\sum_{i=1}^{m}(y_{i..}-y)^2$ does not exceed m-1.

Similarly the ranks of $m\sum_{j=1}^{m}(y_{.j.}-y)^2$ and $m\sum_{k=1}^{m}(y_{..k}-y)^2$ do not exceed m-1. Finally m^2y^2 is of rank one, since

$$m^2y^2 = m^2\left[(1/m^2)\sum_i\sum_j y_{ijk}\right]^2$$

and every element in the matrix of this quadratic form is $1/m^2$.

From (3.25)

$$\sum_{i=1}^{m}\sum_{j=1}^{m} y_{ijk}^2 = Q_a + m\sum_{i=1}^{m}(y_{i..}-y)^2 + m\sum_{j=1}^{m}(y_{.j.}-y)^2 + m\sum_{k=1}^{m}(y_{..k}-y)^2 + m^2y^2.$$

Using Theorem 3.5, we have

$$\begin{aligned} m^2 = r\Big(\sum_i\sum_j y_{ijk}^2\Big) &\leqslant r(Q_a) + r\Big(m\sum_i(y_{i..}-y)^2\Big) + r\Big(m\sum_j(y_{.j.}-y)^2\Big) \\ &\quad + r\Big(m\sum_k(y_{..k}-y)^2\Big) + r(m^2y^2) \\ &\leqslant m^2-3m+2+3(m-1)+1 = m^2. \end{aligned}$$

Hence the equality signs hold throughout the above relation and this is only possible if the quadratic forms

$$m\sum_i(y_{i..}-y)^2,\ m\sum_j(y_{.j.}-y)^2,\ m\sum_k(y_{..k}-y)^2$$

are all of rank m-1.

Hence the rank of $Q_r - Q_a$ is m-1 and, by Theorem 3.1, the statistic to use in our hypothesis $\mu_1 = \mu_2 = \cdots = \mu_m = 0$ is

$$F = \frac{m^2-3m+2}{m-1} \frac{Q_r - Q_a}{Q_a}$$

$$= \frac{m^2-3m+2}{m-1} \frac{m\sum_i y_{i..}^2 - m^2 y^2}{\sum_i \sum_j y_{ijk}^2 - m\left[\sum_i y_{i..}^2 + \sum_j y_{.j.}^2 + \sum_k y_{..k}^2\right] + 2m^2 y^2}$$

This final form of F is the one best adapted to computation.

To test the hypothesis that $\nu_1 = \nu_2 = \cdots = \nu_m = 0$ it is only necessary to replace $m\sum_i y_{i..}^2$ by $m\sum y_{.j.}^2$ in the numerator of F. An analogous change is made for testing the hypothesis $\rho_1 = \rho_2 = \cdots = \rho_k = 0$.

The above results are usually exhibited in the form of an analysis of variance table given by

Source of Variation	Degrees of Freedom	Sum of Squares	Mean Square	F
Rows	m-1	$S_1 = m\sum_i (y_{i..} - y)^2$	$s_1 = S_1/(m-1)$	$F_1 = s_1/s$
Columns	m-1	$S_2 = m\sum_j (y_{.j.} - y)^2$	$s_2 = S_2/(m-1)$	$F_2 = s_2/s$
Varieties	m-1	$S_3 = m\sum_k (y_{..k} - y)^2$	$s_3 = S_3/(m-1)$	$F_3 = s_3/s$
Residual	(m-1)(m-2)	Q_a	$s_4 = Q_a/[(m-1)(m-2)]$	
Total	m^2-1	$\sum_i \sum_j (y_{ijk} - y)^2$		

The value given by the second total follows from (3.25). The statistics used to test the hypotheses $\mu_1 = \mu_2 = \cdots = \mu_m$, $\nu_1 = \nu_2 = \cdots = \nu_m$, $\rho_1 = \rho_2 = \cdots = \rho_m$ are, respectively, F_1, F_2, and F_3.

We shall now test the hypothesis that $\rho_1 = \rho_2$. Since Q_a is unaffected by the change of hypotheses, it remains unchanged. To determine $Q_r - Q_a$ we use Corollary 3.3. Since the hypothesis to be tested may be written $\rho_1 - \rho_2 = 0$, s must be one. From the corollary we see that $\rho_1^* = \rho_1 - \rho_2$ corresponds to β_1^*. The rank of the matrix of coefficients (1,-1) is 1. Since $\hat{\rho}_1$ and $\hat{\rho}_2$ are estimates of ρ_1 and ρ_2 which minimize Q_a we have

$$b_1^* = \hat{\rho}_1 - \hat{\rho}_2 = (y_{..1} - y) - (y_{..2} - y)$$
$$= y_{..1} - y_{..2}.$$

Since $i = j = 1$ the matrix of coefficients (c_{ij}) of $Q_r - Q_a$ is

$$c_{11} = \left(\frac{\sigma_{b_1^*}^2}{\sigma^2}\right)^{-1} = \frac{\sigma^2}{\sigma_{b_1^*}^2}$$

since c_{11} is a one element matrix.

Since $y_{..1}$ and $y_{..2}$ are each the means of m independent observations, we have

$$\sigma_{y_{..1}}^2 = \sum_{ij} (1/m^2)\sigma^2 = \sigma^2/m = \sigma_{y_{..2}}^2.$$

Also $y_{..1}$ and $y_{..2}$ are independent since they are means of two sets of observations which have no observation in common. Hence

$$\sigma_{b_1^*}^2 = \sigma_{y_{..1} - y_{..2}}^2 = (1)^2\sigma^2/m + (-1)^2\sigma^2/m = 2\sigma^2/m.$$

From Corollary 3.3

$$Q_r - Q_a = c_{11} b_1^{*2} = (m/2)(y_{..1} - y_{..2})^2.$$

The number of degrees of freedom of $Q_r - Q_a$ is 1 since it is equal to the rank of the matrix of coefficients (1,-1). Hence to test $\rho_1 = \rho_2$ we have

$$F = \frac{m^2 - 3m - 2}{1} \cdot \frac{m(y_{..1} - y_{..2})^2}{2Q_a}$$

In order to test $\rho_i = 0$ we can use Theorem 3.3 from which

$$Q_r - Q_a = c_{11}(y_{..1} - y_{..2})^2$$

and

$$c_{11} = \frac{\sigma^2}{\sigma^2_{y_{..1} - y_{..2}}}.$$

By definition

$$E(y_{..1}) = (1/m)\sum_{i,j} E(y_{ij1}) = (1/m)\sum_{i,j}(\mu_i + \nu_j + \rho_k + \rho)$$

$$= \rho_1 + \rho,$$

and

$$E(y) = (1/m^2)\sum_{i=1}^{m}\sum_{j=1}^{m} E(y_{ijk}) = (1/m^2)\sum_{i}\sum_{j}(\mu_i + \nu_j + \rho_k + \rho)$$

$$= \rho.$$

Hence

$$E(y_{..1} - y) = E(y_{..1}) - E(y) = \rho_1.$$

Therefore

$$\sigma^2_{y_{..1} - y} = E(y_{..1} - y - \rho_1)^2 = E\left[(y_{..1} - \rho_1 - \rho) - (y - \rho)\right]^2$$

$$= \sigma^2_{y_{..1}} - 2\sigma_{y_{..1}y} + \sigma^2_y.$$

We have that

$$y_{..1} = \sum_{i,j}(1/m) y_{ij1},$$

$$y = \sum_{i}\sum_{j}(1/m^2) y_{ijk}.$$

We now make use of the formula[1]

$$\sigma_{XY} = \sum_{i=1}^{m}\sum_{j=1}^{m}\alpha_i \beta_j \sigma_{x_i x_j}$$

where

---

[1] Wilks p. 34.

$$X = \sum_{i=1}^{m} \alpha_i x_i, \qquad Y = \sum_{j=1}^{m} \beta_j x_j.$$

Since the y_{ijk} are independently distributed

$$\sigma_{y_{..1}y} = \sum_{i,j} (1/m)(1/m^2)\sigma^2_{y_{ij1}} = \sum_{i,j} (1/m^3)\sigma^2 = \sigma^2/m^2.$$

Also

$$\sigma^2_{y_{..1}} = \sigma^2/m, \qquad \sigma^2_{y} = \sigma^2/m^2,$$

since $y_{..1}$ and y are the arithmetic means of m and m^2 terms respectively. Hence

$$\sigma^2_{y_{..1}-y} = \sigma^2(1/m - 2/m^2 + 1/m^2) = \sigma^2(m-1)/m^2,$$

$$c_{11} = \frac{\sigma^2 m^2}{\sigma^2(m-1)} = \frac{m^2}{m-1}.$$

We now have

$$Q_r - Q_a = \frac{m^2}{m-1}(y_{..1} - y)^2.$$

The rank of $Q_r - Q_a$ is the rank of its matrix of coefficients (1) which is 1. Hence, to test $\rho_1 = 0$, we use

$$F = \frac{m^2 - 3m + 2}{1} \cdot \frac{m^2}{m-1} \cdot \frac{(y_{..1} - y_{..2})^2}{Q_a}.$$

Replicated Latin Squares

We shall now apply the above theory to the case where we have r Latin squares. Denote the observations by $y^{(\ell)}_{ijk}$ where ℓ signifies the Latin square under consideration. Our assumption is

$$E(y^{(\ell)}_{ijk}) = \mu^{(\ell)}_i + \nu^{(\ell)}_j + \rho_k + \alpha_{(\ell)} + \beta, \tag{3.39}$$

$$\sum_{i=1}^{m} \mu_i^{(\ell)} = \sum_{j=1}^{m} \nu_j^{(\ell)} = \sum_{k=1}^{m} \rho_k = \sum_{\ell=1}^{r} \alpha_{(\ell)} = 0. \tag{3.40}$$

The quantities $\mu_i^{(\ell)}$, $\nu_j^{(\ell)}$, ρ_k, $\alpha_{(\ell)}$, are called the row, column, varietal, and replicate effects of the ℓth Latin square respectively. To test the hypothesis

$$H: \mu_i^{(\ell)} = 0, \quad i = 1,\ldots,m; \ \ell = 1,\ldots,r,$$

we must first compute Q_a which is the minimum of Q where

$$(3.41) \qquad Q = \sum_{\ell=1}^{r}\sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk}^{(\ell)} - \mu_i^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \rho)^2$$

subject to conditions (3.40). We may write (3.39) as

$$(3.42) \quad E(y_{ijk}^{(\ell)}) = \sum_{\ell'=1}^{r}\sum_{i'=1}^{m}\delta_{\ell\ell'}\delta_{ii'}\mu_{i'}^{(\ell')} + \sum_{\ell'=1}^{r}\sum_{j'=1}^{m}\delta_{jj'}\delta_{\ell\ell'}\nu_{j'}^{(\ell')} + \sum_{k'=1}^{m}\delta_{kk'}\rho_{k'} + \sum_{\ell'=1}^{r}\delta_{\ell\ell'}\alpha_{(\ell')} + \rho$$

Applying Theorem 3.4 where (3.41) is equivalent to $\sum_{i=1}^{p} g_{i\alpha}\beta_i$, and also where $s = mr$, $p = 2mr + m + r + 1$, $\alpha = m^2 r$. We see that (3.41) has the following properties regarding the matrix of coefficients $(g_{i\alpha})$:

(1) every element in the last column is 1, i.e., $g_{p\alpha} = 1$ for all α;

(2) the first s elements in each ~~column~~ row are either zero or one;

(3) the first s columns are orthogonal, since

$$\sum_{\ell=1}^{r}\sum_{i=1}^{m}\sum_{j=1}^{m}\delta_{\ell\ell_1'}\delta_{ii_1'}\delta_{\ell\ell_2'}\delta_{ii_2'} = 0$$

if $\ell_1' \neq \ell_2'$ and, if $\ell_1' = \ell_2'$, is equal to

$$m\sum_{i=1}^{m}\delta_{ii_1'}\delta_{ii_2'} = 0$$

since $i_1' \neq i_2'$;

(4) exactly one of the first s elements in each row has the value one and the rest are zero.

Hence we see that (3.42) satisfies the requirements for Theorem 3.4.

Thus, to find $Q_{\alpha,\beta}$ we may ignore condition (3.40). Minimizing Q in (3.41) we have

$$-\frac{1}{2}\frac{\partial Q}{\partial \mu_i^{(\ell)}} = \sum_{j=1}^{m} (y_{ijk}^{(\ell)} - \mu_i^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \beta) = 0.$$

This reduces to

$$y_{i..}^{(\ell)} - \mu_i^{(\ell)} - \alpha_{(\ell)} - \beta = 0,$$

where $y_{i..}$ is the mean of the observations in the ith row of the ℓth Latin square. Similarly $\partial Q/\partial \nu_j^{(\ell)} = 0$ gives the following equation

$$y_{.j.}^{(\ell)} - \nu_j^{(\ell)} - \alpha_{(\ell)} - \beta = 0,$$

where $y_{.j.}$ is the mean of the observations in the jth column of the ℓth Latin square. Also

$$-\frac{1}{2}\frac{\partial Q}{\partial \rho_k} = \sum_{\ell=1}^{r}\sum_{ij} (y_{ijk}^{(\ell)} - \mu_i^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \beta) = 0.$$

This reduces to

$$y_{..k} - \rho_k - \beta = 0$$

where $y_{..k}$ is the mean of the observations on the kth variety over all the Latin squares. Similarly

$$-\frac{1}{2}\frac{\partial Q}{\partial \alpha_{(\ell)}} = \sum_{i=1}^{m}\sum_{j=1}^{m} (y_{ijk}^{(\ell)} - \mu_i^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \beta) = 0$$

which reduces to

$$y^{(\ell)} - \alpha_{(\ell)} - \beta = 0$$

where $y^{(\ell)}$ is the mean of all the observations in the ℓth Latin square. Finally

$$-\frac{1}{2}\frac{\partial Q}{\partial \beta} = \sum_{\ell=1}^{r}\sum_{i=1}^{m}\sum_{j=1}^{m} (y_{ijk}^{(\ell)} - \mu_i^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \beta) = 0$$

which reduces to

$$y - \beta = 0,$$

where y is the grand mean.

Hence we see that the estimates of $\mu_i^{(\ell)}$, $\nu_j^{(\ell)}$, $\rho_{(k)}$, $\alpha_{(\ell)}$, β,

which minimize Q in (3.41) denoted by $\hat{\mu}_i^{(\ell)}$, $\hat{\nu}_j^{(\ell)}$, $\hat{\rho}_k$, $\hat{\alpha}_{(\ell)}$, $\hat{\rho}$, are

$$
\begin{aligned}
\hat{\mu}_i^{(\ell)} &= y_{i..}^{(\ell)} - y^{(\ell)}, \\
\hat{\nu}_j^{(\ell)} &= y_{.j.}^{(\ell)} - y^{(\ell)}, \\
\hat{\rho}_k &= y_{..k} - y, \\
\hat{\alpha}_{(\ell)} &= y^{(\ell)} - y, \\
\hat{\rho} &= y.
\end{aligned} \tag{3.43}
$$

We can now write Q_a as

$$Q_a = \sum_{\ell=1}^{r} \sum_{i=1}^{m} \sum_{j=1}^{m} (y_{ijk}^{(\ell)} - y_{i..}^{(\ell)} - y_{.j.}^{(\ell)} - y_{..k} + y^{(\ell)} + y)^2$$

Now apply Theorem 3.2 with the following chain of hypotheses,

$$H_1: E(y_{ijk}^{(\ell)}) = \mu_i^{(\ell)} + \nu_j^{(\ell)} + \rho_k + \alpha_{(\ell)} + \rho, \ \sum_i \mu_i^{(\ell)} = \sum_j \nu_j^{(\ell)} = \sum_k \rho_k = \sum_\ell \alpha_{(\ell)} = 0$$

$$H_2: H_1 \ \& \ \mu_i^{(\ell)} = 0, \ i = 1,\ldots,m; \ \ell = 1,\ldots,r,$$

$$H_3: H_2 \ \& \ \nu_j^{(\ell)} = 0, \ j = 1,\ldots,m; \ \ell = 1,\ldots,r, \tag{3.43'}$$

$$H_4: H_3 \ \& \ \rho_k = 0, \ k = 1,\ldots,m,$$

$$H_5: H_4 \ \& \ \alpha_{(\ell)} = 0, \ \ell = 1,\ldots,r.$$

From H_1 we have

$$Y_{ijk}^{(\ell),} = y_{i..}^{(\ell)} + y_{.j.}^{(\ell)} + y_{..k} - y^{(\ell)} - y.$$

Under H_2 we minimize

$$Q = \sum_\ell \sum_i \sum_j (y_{ijk}^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \rho)^2.$$

Thus we have $\partial Q/\partial \nu_j^{(\ell)} = 0$ which gives

$$y_{.j.}^{(\ell)} - \nu_j^{(\ell)} - \alpha_{(\ell)} - \rho = 0. \tag{3.44}$$

Similarly $\partial Q/\partial \rho_k = 0$ reduces to

$$y_{..k} - \rho_k - \rho = 0, \tag{3.45}$$

$\partial Q/\partial \alpha_{(\ell)} = 0$ reduces to

$$y^{(\ell)} - \alpha_{(\ell)} - \rho = 0, \tag{3.46}$$

and $\partial Q/\partial \rho = 0$ reduces to

$$y - \rho = 0. \tag{3.47}$$

Hence from H_2 and (3.44), (3.45), (3.46), and (3.47) we have

$$Y_{ijk}^{(\ell)_2} = y_{.j.}^{(\ell)} + y_{..k} - y.$$

From H_3 and (3.45), (3.46), and (3.47) we have

$$Y_{ijk}^{(\ell)_3} = y_{..k} + y^{(\ell)} - y.$$

From H_4 and (3.46) and (3.47) we have

$$Y_{ijk}^{(\ell)_4} = y^{(\ell)}.$$

Finally from H_5 and (3.47) we have

$$Y_{ijk}^{(\ell)_5} = y.$$

From Theorem 3.2 we have

$$\sum_{\ell}\sum_{i}\sum_{j}(y_{ijk}^{(\ell)})^2 = Q_a + \sum_{\ell}\sum_{i}\sum_{j}(y_{i..}^{(\ell)} - y^{(\ell)})^2 + \sum_{\ell}\sum_{i}\sum_{j}(y_{.j.}^{(\ell)} - y^{(\ell)})^2$$
$$+ \sum_{\ell}\sum_{i}\sum_{j}(y_{..k} - y)^2 + \sum_{\ell}\sum_{i}\sum_{j}(y^{(\ell)} - y)^2 + \sum_{\ell}\sum_{i}\sum_{j} y^2.$$

This may be written

$$\sum_{\ell}\sum_{i}\sum_{j}(y_{ijk}^{(\ell)} - y)^2 = Q_a + m\sum_{\ell}\sum_{i}(y_{i..}^{(\ell)} - y)^2 + m\sum_{\ell}\sum_{j}(y_{.j.}^{(\ell)} - y)^2 \tag{3.48}$$
$$+ mr\sum_{R}(y_{..k} - y)^2 + m^2\sum_{\ell}(y^{(\ell)} - y)^2.$$

Notice that Q_a may be determined from the above relation as all the sums involved can be computed readily for a given problem.

The hypothesis we wish to test now is

$$H: \mu_i^{(\ell)} = 0, \quad i = 1,\ldots,m; \quad \ell = 1,\ldots,r.$$

First we must compute Q_r where Q_r is the minimum of Q in (3.41) under the original assumptions of (3.40) and our present hypothesis.

Hence the expression to be minimized under these conditions becomes

$$Q = \sum_{\ell=1}^{r}\sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk}^{(\ell)} - \nu_j^{(\ell)} - \rho_k - \alpha_{(\ell)} - \rho)^2. \tag{3.49}$$

As before $s = mr$. Since under the present hypothesis we can delete the first r parameters we have that $p = mr + m + r + 1$. By reasoning analogous to the previous case it can be shown that the conditions of Theorem 3.4 hold. This enables us to ignore the conditions

$$\sum_j \nu_j^{(\ell)} = \sum_k \rho_k = \sum_\ell \alpha_{(\ell)} = 0.$$

Minimizing Q in (3.48) we have

$$y_{.j.}^{(\ell)} - \nu_j^{(\ell)} - \alpha_{(\ell)} - \rho = 0,$$
$$y_{..k} - \rho_k - \rho = 0,$$
$$y^{(\ell)} - \alpha_{(\ell)} - \rho = 0,$$

and

$$y - \rho = 0.$$

We see that the estimates of $\nu_j^{(\ell)}$, ρ_k, $\alpha_{(\ell)}$, ρ which are given by $\hat{\nu}_j^{(\ell)}$, $\hat{\rho}_k$, $\hat{\alpha}_{(\ell)}$, $\hat{\rho}$, which minimize Q in (3.48) are the same values of the parameters which determine Q_a. Hence the above estimates are given by (3.43).

Set up the chain of hypothesis H_1', H_2', H_3', H_4', where $H_i' = H_{i+1}$, $i = 1,\ldots,4$, where H_i, $i = 1,\ldots,4$ are given by (3.43′). Applying Theorem 3.2 and using the above hypothesis we have that $Y_{ijk}^{(\ell)_i'}$ $Y_{ijk}^{(\ell)_{(\ell-)}}$, $i = 1,\ldots,4$, where $Y_{ijk}^{(\ell)_i}$ are the regression values used in determining Q_a. We have

$$\sum_\ell\sum_i\sum_j (y_{ijk}^{(\ell)})^2 = Q_r + \sum_\ell\sum_i\sum_j (y_{.j.}^{(\ell)} - y^{(\ell)})^2 + \sum_\ell\sum_i\sum_j (y_{..k} - y)^2 \tag{3.50}$$
$$+ \sum_\ell\sum_i\sum_j (y^{(\ell)} - y)^2 + \sum_\ell\sum_i\sum_j y^2.$$

From (3.50) and (3.48) we have

$$Q_r - Q_a = m \sum_{\ell} \sum_{i} (y_{i..}^{(\ell)} - y^{(\ell)})^2 .$$

From (3.40) we have

$$(3.51) \qquad \mu_m = -\sum_{i'=1}^{m-1} \mu_{i'}^{(\ell)}, \qquad \nu_m^{(\ell)} = -\sum_{j'=1}^{m-1} \nu_{j'}^{(\ell)},$$
$$\rho_m = -\sum_{k'=1}^{m-1} \rho_{k'}, \qquad \alpha_{(n)} = -\sum_{\ell'=1}^{n-1} \alpha_{(\ell')} .$$

From (3.48) and (3.51) we have

$$(3.52) \qquad E(y_{ijk}^{(\ell)}) = \sum_{\ell'=1}^{n} \sum_{i'=1}^{m-1} \delta_{\ell\ell'}(\delta_{ii'} - \delta_{im}) \mu_{i'}^{(\ell)} + \sum_{\ell'=1}^{n} \sum_{j'=1}^{m-1} \delta_{\ell\ell'}(\delta_{jj'} - \delta_{jm}) \nu_{j'}^{(\ell')}$$
$$+ \sum_{k'=1}^{m-1} (\delta_{kk'} - \delta_{km}) \rho_{k'} + \sum_{\ell'=1}^{n-1} (\delta_{\ell\ell'} - \delta_{\ell n}) \alpha_{(\ell')} + \rho .$$

In order to apply Theorem 3.1, to find the rank of Q_a, we need to know the rank of the matrix of the coefficients of the parameters which appear on the right hand side of the equations (3.52). Represent this matrix by the symbol A. First we introduce the following theorems.

Theorem 3.5: If $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ are two sets of linearly independent vectors and each vector of the first set is orthogonal to each vector of the second set so that

$$\alpha_i \cdot \beta_j = 0, \quad i = 1, \ldots, m; \quad j = 1, \ldots, n,$$

then the combined set of vectors $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ is linearly independent.

Proof: Assume there exists constants $c_1, \ldots, c_m, d_1, \ldots, d_n$, such that

$$c_1 \alpha_1 + \ldots + c_m \alpha_m + d_1 \beta_1 + \ldots + d_n \beta_n = 0.$$

Multiplying the above equation by α_i we obtain

$$\sum_{j=1}^{m} c_j (\alpha_i \cdot \alpha_j) = 0.$$

Multiplying the same equation by β_i we obtain

$$\sum_{j=1}^{n} d_j(\beta_i \cdot \beta_j) = 0.$$

This gives a set of $m+n$ homogeneous equations in $m+n$ unknowns. The matrix of coefficients is

$$B = \begin{pmatrix} C & O_1 \\ O_2 & D \end{pmatrix}$$

where C is the $\underline{m}$ x $\underline{m}$ matrix $(\alpha_i \cdot \alpha_j)$, D is the $\underline{n}$ x $\underline{n}$ matrix $(\beta_i \cdot \beta_j)$, O_1 is the $\underline{m}$ x $\underline{n}$ zero matrix, and O_2 is the $\underline{n}$ x $\underline{m}$ zero matrix. We have $|B| = |C||D|$. Also $C = A'A$ where A is the matrix whose column vectors are $\alpha_1, \ldots, \alpha_m$. Since $\alpha_1, \ldots, \alpha_m$ are linearly independent the rank of A is m. Since C is a Gram matrix, its rank is also m. Hence $|C| \neq 0$. Similarly $|D| \neq 0$. Therefore $|B| \neq 0$. Hence the set of homogeneous equations has only the trivial solution

$$c_1 = c_2 = \ldots = c_m = d_1 = d_2 = \ldots = d_n = 0.$$

Thus $\alpha_1, \ldots, \alpha_m, \beta_1, \ldots, \beta_n$ are linearly independent.

Consider the set of column vectors whose elements are the coefficients of $\mu_1^{(\ell')}, \mu_2^{(\ell')}, \ldots, \mu_{m-1}^{(\ell')}$ for a fixed ℓ'. Consider the matrix, A_1 say, whose columns are these vectors. Thus, A_1 is a $\underline{m^2 r}$ x $(\underline{m-1})$ matrix. The elements in the row corresponding to $\ell, i,$ and j are given by $\delta_{\ell\ell'}(\delta_{ii'} - \delta_{im})$ as ℓ' runs from 1 to m-1. This element is zero if $\ell \neq \ell'$ or if $i \neq i'$ or m.

Let $G_1 = A_1'A_1 = (g_{pq})$ be the Gram matrix of A_1. We have

$$g_{pq} = \sum_{\ell=1}^{n} \sum_{i=1}^{m} \sum_{j=1}^{m} (\delta_{\ell\ell'})^2 (\delta_{ip} - \delta_{im})(\delta_{iq} - \delta_{im}) = g_{qp}$$

$$= 2m \text{ if } p = q,$$

$$= m \text{ if } p \neq q.$$

Therefore G_1 is the matrix given by (3.38) of order m-1. From previous work we know that $|G_1| \neq 0$. Hence the rank of G_1 is m-1. Therefore $r(A_1) = m-1$. But the rank of A_1 is the same as the number of columns of A_1. Hence we have that all the columns of A_1 are linearly independent. Thus we may split up the first r(m-1) column vectors of A into r sets of m-1 vectors according to the value of ℓ and each set will be made up of linearly independent vectors.

By an argument similar to the above we can decompose the second set of r(m-1) column vectors into r sets of m-1 linearly independent column vectors.

Denote the matrix of the third block of m-1 vectors by A_2 where A_2 has the dimensions $\underline{m^2 r}$ x $\underline{(m-1)}$. Let $G_2 = A_a' A_a = (g_{pq})$ be the Gram matrix of A_2. The element g_{pq} is given by

$$g_{pq} = \sum_{\ell=1}^{r} \sum_{i=1}^{m} \sum_{j=1}^{m} (\delta_{kp} - \delta_{km})(\delta_{kq} - \delta_{km}) = g_{qp}$$

$$= 2mr \text{ if } p = q,$$

$$= mr \text{ if } p \neq q.$$

As before we see that $|G_2| = r^{m-1} |G_1| \neq 0$. Hence G_2 has rank m-1 which implies that A_2 has rank m-1 also.

Consider the set of r-1 column vectors which are the coefficients of the $\alpha_{(\ell')}$, $\ell' = 1, \ldots, r-1$. Let A_3 be the matrix of coefficients. Thus A_3 has dimensions $\underline{m^2 r}$ x $\underline{(r-1)}$. Denote the Gram matrix of A_3 by $G_3 = A_3' A_3 = (g_{pq})$. The element g_{pq} is given by

$$g_{pq} = \sum_{i=1}^{m} \sum_{j=1}^{m} \sum_{\ell=1}^{r} (\delta_{\ell p} - \delta_{\ell r})(\delta_{\ell q} - \delta_{\ell r}) = g_{qp},$$

$$= 2m^2 \text{ if } p = q,$$

$= m^2$ if $p \neq q$.

Therefore $|G_3| = m^{r-1}|G_1| \neq 0$. Hence G_3 has rank r-1. This implies that $r(A_3) = r-1$.

Since the coefficient of ρ is always 1, we have that the rank of the matrix of coefficients of ρ, say A_4, in (3.53) is 1.

We have broken the matrix A up into $2r+3$ submatrices and the column vectors of each submatrix are linearly independent. We shall show that the column vectors in any submatrix are orthogonal to the column vectors in all the other submatrices. Taking a column vector from two of the first r submatrices and forming their scalar product we have

$$\sum_{\ell} \sum_{i} \sum_{j} (\delta_{\ell\ell_1'})(\delta_{ii'} - \delta_{im})(\delta_{\ell\ell_2'})(\delta_{ii'} - \delta_{im}) = 0$$

since $\ell_1' \neq \ell_2'$. Similarly column vectors selected from any two of the second set of r submatrices are orthogonal.

Next select a column vector from any one of the first r submatrices and a second column vector from any one of the second set of r submatrices and form their scalar product to obtain

$$\sum_{\ell} \sum_{i} \sum_{j} \delta_{\ell\ell_1'}(\delta_{ii'} - \delta_{im}) \cdot \delta_{\ell\ell_2'}(\delta_{jj'} - \delta_{jm}) = 0.$$

Forming the scalar product of a column vector from any of the second set of r submatrices with one from the submatrix formed from the set of m-1 vectors whose elements are the coefficients of the ρ_k's, we have

$$\sum_{\ell} \sum_{i} \sum_{j} \delta_{\ell\ell'}(\delta_{ii'} - \delta_{im}) \cdot (\delta_{kk'} - \delta_{km})$$

$$= \sum_{i} \left[(\delta_{ii'} - \delta_{im}) \sum_{k} (\delta_{kk'} - \delta_{km}) \right] = 0$$

Forming the scalar product of a column vector from any of the first r submatrices with one from the submatrix formed from the set of r-1 vectors whose elements are the coefficients of the $\alpha_{(\ell)}$'s, we have

$$\sum_{\ell} \sum_{i} \sum_{j} \delta_{\ell\ell'}(\delta_{ii'} - \delta_{im}) \cdot (\delta_{\ell\ell'} - \delta_{\ell k}) = 0 .$$

Again forming the scalar product of a column vector from the first set of r submatrices with the column vectors of β we have $\sum_{\ell} \sum_{i} \sum_{j} \delta_{\ell\ell'}(\delta_{ii'} - \delta_{im}) \cdot 1 = 0$.

The above procedure can be repeated with the column vectors from any one of the r submatrices of the second set of r(m-1) column vectors. It can be shown that as before the column vectors in this case are also orthogonal.

Next we shall form the scalar product of any column vector from the submatrix formed from the coefficients of the $\alpha_{(\ell)}$'s with any vector from the submatrix comprising the coefficients of the β_k's. Thus we have

$$\sum_{\ell} \sum_{i} \sum_{k} (\delta_{kk'} - \delta_{km}) \cdot (\delta_{\ell\ell'} - \delta_{\ell k}) = 0 .$$

Also

$$\sum_{\ell} \sum_{i} \sum_{k} (\delta_{kk'} - \delta_{km}) \cdot 1 = 0 .$$

Similarly

$$\sum_{i} \sum_{j} \sum_{\ell} (\delta_{\ell\ell'} - \delta_{\ell k}) \cdot 1 = 0 .$$

Hence we have shown that the sets of column vectors forming the submatrices of A are mutually orthogonal. Thus the 2r(m-1)+m+r-1 column vectors of A are linearly independent. Hence the rank of

A is $2r(m-1)+m+r-1$.

By Theorem 3.1 the rank of Q_a, which is also called its number of degrees of freedom, is

$$m^2r-2r(m-1)-m-r+1=(m-1)(rm-r-1).$$

It remains to determine the rank of

$$Q_r-Q_a=m\sum_{\ell}\sum_{i}(y_{i..}^{(\ell)}-y^{(\ell)})^2.$$

Now Q_r-Q_a is the sum of squares of rm linear relations. We have r linear homogeneous relations among the $y_{i..}^{(\ell)}-y^{(\ell)}$, i.e.,

$$\sum_{i=1}^{m}(y_{i..}^{(\ell)}-y^{(\ell)})=0,\quad \ell=1,\ldots,r.$$

These relations are independent since each $y_{i..}^{(\ell)}-y^{(\ell)}$ appears in only one equation. Therefore by Theorem 3.5 we have

$$r\left[m\sum_{\ell=1}^{k}\sum_{i=1}^{m}(y_{i..}^{(\ell)}-y^{(\ell)})^2\right]\leq rm-r.$$

Similarly

$$r\left[m\sum_{j=1}^{m}\sum_{\ell=1}^{k}(y_{.j.}^{(\ell)}-y^{(\ell)})^2\right]\leq rm-r.$$

Also

$$r\left[mr\sum_{k=1}^{m}(y_{..k}-y)^2\right]\leq m-1,$$

and

$$r\left[m^2\sum_{\ell=1}^{k}(y^{(\ell)}-y)^2\right]\leq r-1.$$

The rank of $\sum_{\ell}\sum_{i}\sum_{j}y^2$ is 1.

From (3.48) and Theorem 3.5 we have that

$$\begin{aligned}m^2r=r\left[\sum_{\ell}\sum_{i}\sum_{j}(y_{ijk}^{(\ell)})^2\right]&\leq r[Q_a]+r\left[m\sum_{\ell}\sum_{i}(y_{i..}^{(\ell)}-y^{(\ell)})^2\right]\\&+r\left[m\sum_{\ell}\sum_{i}(y_{.j.}^{(\ell)}-y^{(\ell)})^2\right]+r\left[mr\sum_{k}(y_{..k}-y)^2\right]\\&+r\left[m^2\sum_{\ell}(y^{(\ell)}-y)^2\right]+r\left[\sum_{\ell}\sum_{i}\sum_{j}y^2\right]=m^2r\end{aligned}$$

Hence the equality signs must hold throughout. Thus the quadratic form $Q_r - Q_a$ must have rank $r(m-1)$, and the ranks of the other quadratic forms are also determined.

To test the hypothesis $\mu_i^{(\ell)} = 0$, $i = 1,\ldots,m$; $\ell = 1,\ldots,r$, the appropriate statistic to use is, by Theorem 3.1,

$$(3.53) \qquad F_1 = \frac{(m-1)(rm-r-1)}{r(m-1)} \cdot \frac{Q_r - Q_a}{Q_a}$$

$$= \frac{(rm-r-1)}{r} \cdot \frac{m\sum_{\ell}\sum_{i}(y_{i\cdot\cdot}^{(\ell)})^2 - m^2\sum_{\ell}(y^{(\ell)})^2}{\sum_{\ell}\sum_{i}\sum_{j}(y_{ijk}^{(\ell)})^2 - m\left[\sum_{\ell}\sum_{i}(y_{i\cdot\cdot}^{(\ell)})^2 + \sum_{\ell}\sum_{j}(y_{\cdot j\cdot}^{(\ell)})^2 + r\sum_{k}(y_{\cdot\cdot k})^2 - m\sum_{\ell}(y^{(\ell)})^2 + m^2 r y^2\right]}$$

The final form of F_1 is the one best adapted to computational purposes.

The statistics for testing the hypotheses $\nu_j^{(\ell)} = 0$, $j = 1,\ldots,m$, $\ell = 1,\ldots,r$; $\beta_k = 0$, $k = 1,\ldots,m$; $\alpha^{(\ell)} = 0$, $\ell = 1,\ldots,r$, are respectively

$$F_2 = \frac{(rm-r-1)}{r} \cdot \frac{m\sum_{\ell}\sum_{j}(y_{\cdot j\cdot}^{(\ell)} - y^{(\ell)})^2}{Q_a},$$

$$F_3 = \frac{(rm-r-1)}{1} \cdot \frac{mr\sum_{k}(y_{\cdot\cdot k} - y)^2}{Q_a},$$

$$F_4 = \frac{(m-1)(rm-r-1)}{r-1} \cdot \frac{m^2\sum_{\ell}(y^{(\ell)} - y)^2}{Q_a},$$

where Q_a is given in (3.53). These results can be expressed compactly in the following analysis of variance table:

Source of Variation	Degrees of Freedom	Sum of Squares	Mean Square	F
Rows	$r(m-1)$	$S_1 = m\sum_{\ell=1}^{r}\sum_{i=1}^{m}(y_{i..}^{(\ell)} - y^{(\ell)})^2$	$s_1 = S_1/r(m-1)$	$F_1 = s_1/s_5$
Columns	$r(m-1)$	$S_2 = m\sum_{\ell=1}^{r}\sum_{j=1}^{m}(y_{.j.}^{(\ell)} - y^{(\ell)})^2$	$s_2 = S_2/r(m-1)$	$F_2 = s_2/s_5$
Varieties	$m-1$	$S_3 = mr\sum_{k=1}^{m}(y_{..k} - y)^2$	$s_3 = S_3/(m-1)$	$F_3 = s_3/s_5$
Replications	$r-1$	$S_4 = m^2\sum_{\ell=1}^{r}(y^{(\ell)} - y)^2$	$s_4 = S_4/(r-1)$	$F_4 = s_4/s_5$
Residual	$(m-1)(mr-r-1)$	Q_a	$s_5 = Q_a/[(m-1)(mr-r-1)]$	
Total	m^2r	$\sum_{\ell}\sum_{i}\sum_{j}(y_{ijk}^{(\ell)} - y)^2$		

The value of the second total follows from (3.48).

ORTHOGONAL LATIN SQUARES

We shall now extend the theory presented in the previous sections to the case where we have r orthogonal Latin squares of side m where $r \leq m-1$. Denote the observations by $y_{ijk_1,\ldots k_r}$ where $i,j = 1,\ldots,m$ denote the row and column numbers respectively and k_s, $s = 1,\ldots,r$, take on the values from 1 to m. Our assumptions are

$$E(y_{ijk_1,\ldots k_r}) = \mu_i + \nu_j + \rho_{k_1}^{(1)} + \rho_{k_2}^{(2)} + \cdots + \rho_{k_r}^{(r)} + \rho, \tag{3.54}$$

$$\sum_{i=1}^{m}\mu_i = \sum_{j=1}^{m}\nu_j = \sum_{k_1=1}^{m}\rho_{k_1}^{(1)} = \cdots = \sum_{k_r=1}^{m}\rho_{k_r}^{(r)} = 0, \tag{3.55}$$

The subscripts k_ℓ, $\ell = 1,\ldots,r$ are functions of i and j such that for a fixed i (j) they take on each of the values from 1 to m exactly once in some order as j (i) takes on the values from 1 to m.

Also the pair of numbers (k_ℓ, k_m) takes on every possible ordered pair of numbers exactly once where k_ℓ and k_m are selected independently from the numbers 1 to m. The parameters μ_i, ν_j, $\rho_{k_\ell}^{(\ell)}$, $\ell = 1,\ldots,r$, represent the row, column, and varietal effects respectively.

In order to test the hypothesis

$H: \mu_i = 0,\ i = 1,\ldots,m,$

we must first compute Q_a which is the minimum of Q subject to conditions (3.55) where

$$(3.56) \qquad Q = \sum_{i=1}^{m}\sum_{j=1}^{m}(y_{ijk_1\ldots k_r} - \mu_i - \nu_j - \rho_{k_1}^{(1)} - \rho_{k_2}^{(2)} - \rho_{k_r}^{(r)} - \rho)^2$$

As in the previous section, we may again show that (3.56) satisfies Theorem 3.4 where $s = m$, $p = 2m+mr+1$, and $\alpha = m^2$. Thus to find Q_a we may ignore the conditions of (3.55). Hence $\partial Q/\partial \mu_i = 0$ reduces to

$$y_i - \mu_i - \rho = 0,$$

and $\partial Q/\partial \nu_j = 0$ reduces to

$$y_j - \nu_j - \rho = 0,$$

where y_i and y_j are the means of the observations of the ith row and jth columns respectively. Also we have

$$\frac{\partial Q}{\partial \rho_{k_\ell}^{(\ell)}} = \sum_{ijk_\ell}(y_{ijk_1\ldots k_r} - \mu_i - \nu_j - \rho_{k_1}^{(1)} - \ldots \rho_{k_r}^{(r)} - \rho) = 0$$

where $\sum_{ijk_\ell}$ means summation over the m pairs of values for i and j which give us terms involving $\rho_{k_\ell}^{(\ell)}$. The equation reduces to

$$y_{k_\ell}^{(\ell)} - \rho_{k_\ell}^{(\ell)} - \rho = 0,$$

where $y_{k_\ell}^{(\ell)}$ is the average of the m values of $y_{ijk_1,\ldots,k_r}$ which have

the given number k as the $(\ell+2)$nd subscript. The expression $\sum_{i,j,k_\ell} \rho_{k_n}^{(n)}$ vanishes in the above relation since k_ℓ appears with each value of k_n exactly once, i.e.,

$$\sum_{i,j,k_\ell} \rho_{k_n}^{(n)} = \sum_{k_n=1}^{m} \rho_{k_n}^{(n)} = 0 .$$

Finally

$$\frac{\partial Q}{\partial \rho} = y - \rho = 0.$$

Thus the estimates of μ_i, ν_j, $\rho_{k_\ell}^{(\ell)}$ and ρ which minimize (3.56), denoted by $\hat{\mu}_i$, $\hat{\nu}_j$, $\hat{\rho}_{k_\ell}^{(\ell)}$, and $\hat{\rho}$, are,

$$\begin{aligned} \hat{\rho} &= y, \\ \hat{\rho}_{k_\ell}^{(\ell)} &= y_{k_\ell}^{(\ell)} - y, \\ \hat{\nu}_j &= y_j - y, \\ \hat{\mu}_i &= y_i - y. \end{aligned} \tag{3.57}$$

We may write Q_a as

$$Q_a = \sum_{i=1}^{m} \sum_{j=1}^{m} \left(y_{ijk_1,\ldots,k_r} - y_i - y_j - y_{k_1}^{(1)} - y_{k_2}^{(2)} - \cdots - y_{k_r}^{(r)} + (r+1)y \right)^2 .$$

Now apply Theorem 3.2 with the following chain of hypotheses,

$$\begin{aligned} &H_1: \ E(y_{ijk_1,\ldots,k_r}) = \mu_i + \nu_j + \rho_{k_1}^{(1)} + \cdots + \rho_{k_r}^{(r)} + \rho, \ \sum_i \mu_i = \sum_j \nu_j = \sum_{k_1} \rho_{k_1}^{(1)} = \cdots = \sum_{k_r} \rho_{k_r} = \\ &H_2: \ H_1 \ \& \ \mu_i = 0, \ i = 1,\ldots,m, \\ &H_3: \ H_2 \ \& \ \nu_j = 0, \ j = 1,\ldots,m, \\ &H_4: \ H_3 \ \& \ \rho_{k_r}^{(r)} = 0, \ k_r = 1,\ldots,m, \\ &\qquad \cdots \\ &H_{r+3}: \ H_{r+2} \ \& \ \rho_{k_1}^{(1)} = 0, \ k_r = 1,\ldots,m. \end{aligned} \tag{3.57'}$$

From H_1 we have

$$Y^{(1)} = y_i + y_j + y^{(1)}_{k_1} + y^{(2)}_{k_2} + \cdots + y^{(r)}_{k_\ell} - (r+1)y$$

$$= y_i + y_j + \sum_{\ell=1}^{r} y^{(\ell)}_{k_\ell} - (r+1)y.$$

Under H_2 we minimize

$$Q = \sum_i \sum_j (y_{ijk_1,\ldots,k_\ell} - \nu_j - \rho^{(1)}_{k_1} - \cdots - \rho^{(r)}_{k_r} - \rho)^2$$

Thus we have $\partial Q/\partial \nu_j = 0$ which gives

(3.58) $$y_j - \nu_j - \rho = 0.$$

Similarly $\partial Q/\partial \rho_{k_\ell} = 0$ reduces to

(3.59) $$y^{(\ell)}_{k_\ell} - \rho^{(\ell)}_{k_\ell} - \rho = 0, \quad \ell = 1,\ldots,r,$$

and $\partial Q/\partial \rho = 0$ reduces to

(3.60) $$y - \rho = 0.$$

From H_2 and (3.58), (3.59), and (3.60) we have

$$Y^{(2)} = y_j - y + \sum_{\ell=1}^{r} (y^{(\ell)}_{k_\ell} - y) + y$$

$$= y_j + \sum_{\ell=1}^{r} y^{(\ell)}_{k_\ell} - ry.$$

From H_3 and (3.59) and (3.60) we have

$$Y^{(3)} = \sum_{\ell=1}^{k} (y^{(\ell)}_{k_\ell} - y) + y$$

$$= \sum_{\ell=1}^{k} y^{(\ell)}_{k_\ell} - (r-1)y.$$

From H_4 and (3.59) and (3.60)

$$Y^{(4)} = \sum_{\ell=1}^{r-1} (y^{(\ell)}_{k_\ell} - y) + y$$

$$= \sum_{\ell=1}^{r-1} y^{(\ell)}_{k_\ell} - (r-2)y.$$

From H_5 and (3.59) and (3.60)

$$Y^{(5)} = \sum_{\ell=1}^{k-2}(y_{k_\ell}^{(\ell)} - y) + y$$
$$= \sum_{\ell=1}^{k-2} y_{k_\ell}^{(\ell)} - (r-3)y.$$

Following through in the same fashion with the remainder of the hypotheses we have from H_{r+2} and (3.59) and (3.60)

$$Y^{(r+2)} = y_{k_1}^{(1)}.$$

Finally we have, under H_{r+3} and (3.60),

$$Y^{(r+3)} = y.$$

From Theorem 3.2 we have

$$\sum_i \sum_j y^2_{ijk_1,\ldots,k_k} = Q_a + \sum_i \sum_j (y_i - y)^2 + \sum_i \sum_j (y_j - y)^2 + \sum_\ell \sum_i \sum_j (y_{k_\ell}^{(\ell)} - y)^2 + \sum_i \sum_j y^2.$$

This may be written

$$\sum_i \sum_j (y_{ijk_1,\ldots,k_k} - y)^2 = Q_a + m \sum_i (y_i - y)^2 + m \sum_j (y_j - y)^2 + m \sum_\ell \sum_{k_\ell} (y_{k_\ell}^{(\ell)} - y)^2. \tag{3.61}$$

Since all the sums appearing in the above equation are readily computed, Q_a may be determined from (3.61).

The hypothesis we wish to test now is

$H: \mu_i = 0, \quad i = 1,\ldots,m.$

First we must compute Q_r where Q_r is the minimum of Q in (3.56) under the original assumptions of (3.55) and our present hypothesis. Hence the expression to be minimized under these conditions becomes

$$Q = \sum_i \sum_j (y_{ijk_1,\ldots k_k} - \nu_j - \rho_{k_1}^{(1)} - \ldots - \rho_{k_k}^{(k)} - \rho)^2. \tag{3.62}$$

As before $s = m$. From our present hypothesis we have that $p = m+mr+1$. As before we can show that the conditions of Theorem 3.4 hold. Hence we may ignore the conditions $\sum_{j=1}^{m} \nu_j = 0$, $\sum_{k_\ell=1}^{m} \rho_{k_\ell}^{(\ell)} = 0$, $\ell = 1,\ldots,r$. Thus, minimizing Q in (3.62) we have

$$y_j - \nu_j - \rho = 0,$$

$$y_{k_\ell}^{(\ell)} - \rho_{k_\ell}^{(\ell)} - \rho = 0,$$

and

$$y - \rho = 0.$$

We see that the estimates of ν_j, $\rho_{k_\ell}^{(\ell)}$ and ρ which minimize Q in (3.62) are given by (3.57).

Set up the hypotheses $H_1', H_2', \ldots, H_{r+2}'$, where $H_i' = H_{i+1}$, $i = 1,\ldots,r+2$, are given by (3.57'). Hence we have

$$(3.63) \qquad \sum_i \sum_j y_{ijk_1\ldots k_\ell}^2 = Q_r + \sum_i \sum_j (y_j - y)^2 + m \sum_\ell \sum_{k_\ell} (y_{k_\ell}^{(\ell)} - y)^2 + \sum_i \sum_j y^2.$$

From (3.61) and (3.63) we have

$$Q_r - Q_a = m \sum_i (y_i - y)^2.$$

From (3.55) we have

$$(3.64) \qquad \mu_m = -\sum_{i'=1}^{m-1} \mu_{i'}, \quad \nu_m = -\sum_{j'=1}^{m-1} \nu_{j'}, \quad \rho_m^{(\ell)} = -\sum_{k_\ell'=1}^{m-1} \rho_{k_\ell'}^{(\ell)}.$$

From (3.54) and (3.64) we have

$$(3.65) \qquad E(y_{ijk_1\ldots k_\ell}) = \sum_{i'=1}^{m-1} (\delta_{ii'} - \delta_{im}) \mu_{i'} + \sum_{j'=1}^{m-1} (\delta_{jj'} - \delta_{jm}) \nu_{j'} + \sum_{\ell=1}^{k} \sum_{k_\ell'=1}^{m-1} (\delta_{k_\ell k_\ell'} - \delta_{k_\ell m}) \rho_{k_\ell}^{(\ell)} + \rho.$$

In order to apply Theorem 3.1, to find the rank of Q_a, we need to know the rank of the matrix of the coefficients of the parameters

which appear on the right hand side of equation (3.65). Represent this matrix by the symbol A.

Consider the set of column vectors whose elements are the coefficients of $\mu_{i'}$, $i' = 1,\ldots,m-1$. These form a matrix, A_1, which has m^2 rows and m-1 columns. Denote the Gram matrix of A_1 by $G_1 = A_1'A_1 = (g_{pq})$, where $p,q = 1,\ldots,m-1$. Hence

$$g_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{ip} - \delta_{im})(\delta_{iq} - \delta_{im}) = g_{qp}$$

$$= 2m \text{ if } p = q,$$

$$= m \text{ if } p \neq q.$$

Therefore the matrix G_1 is given by (3.38), and is of order m-1. From previous work we know that $|G_1| \neq 0$. Hence the rank of G_1 is m-1. Therefore $r(A_1) = m-1$. Hence the m-1 columns of A_1 are linearly independent.

By an argument similar to the above we can show that the m-1 column vectors whose elements are the coefficients of $\nu_{j'}$, $j' = 1,\ldots,m-1$, are also linearly independent.

Consider next the matrix of the r(m-1) coefficients of the $\rho_{k\ell}$'s. Split up these r(m-1) vectors into r sets of m-1 vectors according to the value of ℓ. For $\ell = \ell_1$ denote the matrix of coefficients by A_2 and its Gram matrix by $G_2 = A_2'A_2 = (g_{pq})$ where $p,q = 1,\ldots,m-1$. Hence

$$g_{pq} = \sum_{i=1}^{m}\sum_{j=1}^{m}(\delta_{k_{\ell_1}i} - \delta_{k\ell_1 m})(\delta_{k_{\ell_1}j} - \delta_{k\ell_1 m}) = g_{qp}$$

$$= \sum_{i=1}^{m}\sum_{k_{\ell_1}=1}^{m}(\delta_{k_{\ell_1}p} - \delta_{k\ell_1 m})(\delta_{k_{\ell_1}q} - \delta_{k\ell_1 m})$$

$$= 2m \text{ if } p = q,$$

$$= m \text{ if } p \neq q.$$

Thus $G_2 = G_1$. Hence the m-1 columns of A_2 are linearly independent. Thus each of the r sets consists of linearly independent vectors.

Since the coefficient of ρ is always 1 the rank of the matrix, consisting of the coefficients of ρ, is 1.

We have broken the matrix A up into r+3 submatrices and have shown that the column vectors of each submatrix are linearly independent. We shall now show that the column vectors in any submatrix are orthogonal to the column vectors in all the other submatrices. Taking a column vector from the first submatrix and forming the scalar product with a column vector from the second submatrix we have

$$\sum_i \sum_j (\delta_{ii'} - \delta_{im}) \cdot (\delta_{jj'} - \delta_{jm}) = 0.$$

Forming the scalar product of a column vector from the first submatrix with a vector from any submatrix of the r submatrices which are the coefficients of the ρ_{k_ℓ}'s we have

$$\sum_{i=1}^{m} \sum_{j=1}^{m} (\delta_{ii'} - \delta_{im}) \cdot (\delta_{k_\ell k_\ell'} - \delta_{k_\ell m})$$

$$= \sum_{i=1}^{m} \sum_{k_\ell=1}^{m} (\delta_{ii'} - \delta_{im}) \cdot (\delta_{k_\ell k_\ell'} - \delta_{k_\ell m}) = 0 .$$

Repeating this process with the coefficient of ρ we have

$$\sum_i \sum_j (\delta_{ii'} - \delta_{im}) \cdot 1 = 0 .$$

A similar proof holds if we replace the vector from the first submatrix by a vector from the second submatrix.

Taking any two column vectors from any two submatrices whose elements are the coefficients of the ρ_{k_ℓ}'s we have

$$\sum_{k_\ell=1}^{m}\sum_{k_n=1}^{m}(\delta_{k_\ell k_{\ell'}}-\delta_{k_\ell m})\cdot(\delta_{k_n k_{\ell_2}'}-\delta_{k_n m})=0$$

since as i and j independently take on the values $1,2,\ldots,m$, k_ℓ and k_n take on all the possible m^2 pairs of values selected from $1,2,\ldots,m$ exactly once.

Finally we have

$$\sum_i\sum_j(\delta_{k_\ell k_{\ell'}}-\delta_{k_\ell m})\cdot 1$$

$$=\sum_i\sum_{k_\ell}(\delta_{k_\ell k_{\ell'}}-\delta_{k_\ell m})\cdot 1=0.$$

Hence we have shown that the sets of column vectors forming the submatrices of A are mutually orthogonal. Thus the $2(m-1)+r(m-1)+1$ columns of A are linearly independent. Hence the rank of A is $2m+r(m-1)-1$.

By Theorem 3.1 the rank of Q_a is

$$m^2-2m-r(m-1)+1=(m-1)(m-r-1).$$

It remains to determine the rank of

$$Q_r-Q_a=m\sum_i(y_i-y)^2.$$

Now Q_r-Q_a is the sum of squares of m linear forms. We have a linear homogeneous relation such that

$$\sum_i(y_i-y)=0.$$

Thus by Theorem 3.5 we have that

$$r\left[m\sum_i(y_i-y)^2\right]\leq m-1.$$

Similarly

$$r\left[m\sum_i(y_j-y)^2\right]\leq m-1.$$

Now $m\sum_\ell\sum_{k_\ell}(y_{k_\ell}^{(\ell)}-y)^2$ is the sum of squares of mr linear forms. We

have r linear homogeneous relations of the form

$$\sum_{k_\ell=1}^{m}(y_{k_\ell}^{(\ell)}-y)=0, \quad \ell=1,\ldots,r.$$

These relations are linearly independent in the $(y_{k_\ell}^{(\ell)}-y)$'s since every $y_{k_\ell}^{(\ell)}-y$ appears in only one equation. Thus by Theorem 3.5 we have

$$r\left[m\sum_{\ell}\sum_{k_\ell}(y_{k_\ell}^{(\ell)}-y)^2\right]\leqslant r(m-1).$$

The rank of $\sum_i\sum_j y^2$ is 1. From (3.61) and Theorem 3.5 we have

$$\begin{aligned}m^2=r\left[\sum\sum y_{ijk_1\ldots k_r}^2\right]&\leqslant r\left[Q_a\right]+r\left[m\sum_i(y_i-y)^2\right]+r\left[m\sum_j(y_j-y)^2\right]\\&\quad+r\left[m\sum_\ell\sum_{k_\ell}(y_{k_\ell}^{(\ell)}-y)^2\right]+\left[r\sum_i\sum_j y^2\right]\\&\leqslant m^2-2m-rm+r+1+2(m-1)+r(m-1)+1=m^2.\end{aligned}$$

Hence the equality signs must hold throughout. Thus the quadratic form $Q_r - Q_a$ must have rank m-1, and the ranks of the other forms are also determined.

To test the hypothesis $\mu_i=0$, $i=1,\ldots,m$, the appropriate statistic to use is, by Theorem 3.1,

$$(3.66)\qquad F_1\approx\frac{(m-1)(m-r-1)}{m-1}\cdot\frac{Q_r-Q_a}{Q_a}$$

$$=(m-r-1)\cdot\frac{m\sum_i y_i^2-m^2y^2}{\sum_i\sum_j y_{ijk_1\ldots k_r}^2-m\left[\sum_i y_i^2+\sum_j y_j^2+\sum_\ell\sum_{k_\ell}(y_{k_\ell}^{(\ell)})^2\right]+m^2(r+1)y^2}$$

where F_1 has the F- distribution with m-1 and (m-1)(m-r-1) degrees of freedom.

The statistics for testing the hypotheses $\nu_j=0$, $j=1,\ldots,m$; $\rho_{k_\ell}^{(\ell)}=0$, $k_\ell=1,\ldots,m$, $\ell=1,\ldots,r$, are respectively

$$F_2 = (m-r-1)\cdot \frac{m\sum_j y_j^2 - m^2 y^2}{Q_a},$$

$$F_3 = (m-r-1)\cdot \frac{m\sum_{k_1}(y_{k_1}^{(1)})^2 - m^2 y^2}{Q_a},$$

$$F_4 = (m-r-1)\cdot \frac{m\sum_{k_2}(y_{k_2}^{(2)})^2 - m^2 y^2}{Q_a},$$

$$\cdots\cdots\cdots$$

$$F_{r+2} = (m-r-1)\cdot \frac{m\sum_{k_r}(y_{k_r}^{(r)})^2 - m^2 y^2}{Q_a},$$

where Q_a is given in (3.66), and the number of degrees of freedom associated with each F are m-1 and (m-1)(m-r-1).

CHAPTER IV

THE ANALYSIS OF INCOMPLETE BALANCED BLOCK DESIGNS

We recall that an incomplete balanced block design is an arrangement of v varieties into b blocks of k plots each such that:

(1) no block contains the same variety twice;

(2) every variety is replicated r times;

(3) every variety v_i occurs with every other variety v_j exactly λ times in the same block.

We also have two important relations governing an incomplete balanced block design, viz., $kb = rv$, and $r(k-1) = \lambda(v-1)$.

Denote by y_{ij} the yield of variety i when planted in block j, $i = 1,\ldots,v$; $j = 1,\ldots,b$. Let n_{ij} (which is 0 or 1) be the number of times variety i occurs in block j. Then

$$(4.1) \qquad \sum_{i=1}^{v} n_{ij} = k, \qquad \sum_{j=1}^{b} n_{ij} = r,$$

where k is the number of plots in a block and r is the number of replications of each variety. Also

$$(4.2) \qquad \sum n_{ij} n_{\ell j} = \left\{ \begin{matrix} \lambda, & \ell \neq i \\ r, & \ell = i \end{matrix} \right\} = \lambda + \delta_{\ell i}(r-\lambda),$$

where λ is the number of times each pair of varieties appears together in the same block. Thus we have

$$(4.3) \qquad E(y_{ij}) = n_{ij}(v_i + b_j + \mu),$$

where

$$\sum_{i=1}^{r} v_i = \sum_{j=1}^{b} b_j = 0, \tag{4.4}$$

where v_i and b_j are the varietal and block effects respectively.

In order to test the hypothesis $v_i = 0$, $i = 1, \ldots, v$, we must determine Q_a which is the minimum of Q, where

$$Q = \sum_{i=1}^{r} \sum_{j=1}^{b} n_{ij} (y_{ij} - v_i - b_j - \mu)^2, \tag{4.5}$$

subject to the conditions (4.4). Checking off the assumptions of Theorem 3.4 we have that

(1) μ is the general mean,

(2) the coefficients of the v_i are either zero or one.

Although (4.3) appears to be vb equations, the actual number is kb (recalling that $v > k$). However in the mythical equations the coefficients of the remaining $b(v-k)$ equations are all zero and a row of zeros does not affect the rank of the matrix of coefficients. Hence we may use the "enlarged" matrix and to verify condition (3) we wish to show that the v_i columns are orthogonal. A given row corresponds to a pair of values for i and j. The portion of the row corresponding to the first v columns either contains nothing but zeros or a single 1 in the v_ith column. Thus conditions (3) and (4) hold. Hence we may ignore the conditions of (4.4) in determining Q_a. Thus

$$\begin{aligned} \frac{\partial Q}{\partial \mu} &= \sum_i \sum_j n_{ij} y_{ij} - \sum_i v_i \sum_j n_{ij} - \sum_j b_j \sum_i n_{ij} - \sum_i \sum_j n_{ij} \mu \\ &= G - r \sum_i v_i - k \sum_j b_j - rv\mu \\ &= G - rv\mu = 0 \end{aligned}$$

where G is the total yield. Hence $\hat{\mu} = y$, where y is the grand mean.

Similarly

$$\frac{\partial Q}{\partial v_i} = \sum_{j=1}^{b} n_{ij}(y_{ij} - v_i - b_j - \mu)$$

$$= \sum_{j=1}^{b} n_{ij} y_{ij} - v_i \sum_{j=1}^{b} n_{ij} - \sum_{j=1}^{b} n_{ij} b_j - \mu \sum_j n_{ij}$$

$$= V_i - r v_i - \sum_j n_{ij} b_j - r\mu = 0.$$

Hence

$$V_i = r\hat{v}_i + \sum_{j=1}^{b} n_{ij} \hat{b}_j + ry \tag{4.6}$$

where $V_i = \sum_{j=1}^{b} n_{ij} y_{ij}$ is the total yield of the ith variety.

Also

$$\frac{\partial Q}{\partial b_j} = \sum_{i'=1}^{r} n_{ij}(y_{ij} - v_i - b_j - \mu)$$

$$= \sum_{i'=1}^{r} n_{i'j} y_{i'j} - \sum_{i'=1}^{r} n_{i'j} v_i - k b_j - k\mu = 0.$$

Hence

$$B_j = \sum_{i'=1}^{r} n_{i'j} \hat{v}_{i'} + k\hat{b}_j + ky \tag{4.7}$$

where $B_j = \sum_{i'=1}^{r} n_{i'j} y_{i'j}$ is the sum of the yields of the varieties planted in the jth block. Let $T_i = \sum_{j=1}^{b} n_{ij} B_j$ be the sum of the totals of all blocks containing the ith variety.

Multiply (4.7) by n_{ij} and sum with respect to j to obtain

$$T_i = \sum_{j=1}^{b} \sum_{i'=1}^{r} n_{i'j} n_{ij} \hat{v}_{i'} + k \sum_{j=1}^{b} n_{ij} \hat{b}_j + rky \tag{4.8}$$

$$= \sum_{i'=1}^{r} \left[\lambda + \delta_{ii'}(r - \lambda) \right] \hat{v}_{i'} + k \sum_{j=1}^{b} n_{ij} \hat{b}_j + rky$$

$$= (r - \lambda)\hat{v}_i + k \sum_{j=1}^{b} n_{ij} \hat{b}_j + rky.$$

Multiply (4.6) by k and subtract (4.8) from it to obtain

$$kV_i - T_i = (kr - r + \lambda)\hat{v}_i. \tag{4.9}$$

But $kr - r + \lambda = r(k-1) + \lambda = \lambda(v-1) + \lambda = \lambda v$. Hence (4.9) may be written

$$\hat{v}_i = \frac{kV_i - T_i}{\lambda v}. \tag{4.10}$$

Substituting in (4.7) we have

$$\hat{b}_j = (1/k)B_j - (1/k\lambda v)\sum_{i=1}^{v} n_{ij}(kv_i - T_i) - y.$$

Consider the chain of hypotheses :

H_1: $E(y_{ij}) = n_{ij}(v_i + b_j + \mu)$, $\sum_i v_i = \sum_j b_j = 0$;

H_2: H_1 & $v_i = 0$, $i = 1,\ldots,v$;

H_3: H_2 & $b_j = 0$, $j = 1,\ldots,b$.

Under H_2 consider the effect of the condition $\sum_j b_j = 0$. Conditions (1) and (2) in Theorem 3.4 are satisfied immediately. Also any row corresponds to a definite block number. There will be a 1 in the column corresponding to the block number and zeros in the columns corresponding to the remaining blocks. Hence conditions (3) and (4) of the theorem hold true also. Thus we may ignore the condition $\sum_j b_j = 0$.

From H_1 we have

$$Y_{ij}^{(1)} = \hat{v}_i + \hat{b}_j + \mu$$

$$= \frac{1}{\lambda v}(kV_i - T_i) + \frac{1}{k}B_j - \frac{1}{k}\sum_{i'=1}^{v} n_{i'j}\hat{v}_i.$$

To determine $Y_{ij}^{(2)}$, under H_2 we see that we must minimize

$$Q = \sum_{i=1}^{v}\sum_{j=1}^{b} n_{ij}(y_{ij} - b_j - \mu)^2.$$

We have $\partial Q/\partial b_j = 0$ which reduces to

$$\hat{b}_j = \frac{B_j}{k} - y.$$

Also from $\partial Q/\partial \mu = 0$ we obtain again $\hat{\mu} = y$. Hence

$$Y_{ij}^{(2)} = \frac{B_j}{k}.$$

Finally we have that $Y_{ij}^{(3)} = y$. Then

$$(4.12) \quad \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij} y_{ij}^2 = Q_a + \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij}\left[v_i - \frac{1}{k}\sum_{i'=1}^{r} n_{i'j}\hat{v}_{i'}\right]^2 + \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij}\left(\frac{B_j}{k} - y\right)^2 + kby^2.$$

Now

$$\sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij}\left(\frac{B_j}{k} - y\right)^2 = k\sum_{j=1}^{b}\left(\frac{B_j}{k} - y\right)^2 = \frac{1}{k}\sum_{j=1}^{b} B_j^2 - 2y\sum_{j=1}^{b} B_j + kby^2$$

$$= \frac{1}{k}\sum_{j=1}^{b} B_j^2 - kby^2.$$

Then

$$(4.13) \quad Q_a = \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij} y_{ij}^2 - \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij}\left[\hat{v}_i - \frac{1}{k}\sum_{i'=1}^{r} n_{i'j}\hat{v}_{i'}\right]^2 - \frac{1}{k}\sum_{j=1}^{b} B_j^2.$$

We wish to test the hypothesis: $v_1 = v_2 = \ldots = v_v = 0$.

Renaming the above chain of hypotheses as $H_1' = H_2$, $H_2' = H_3$, we have

$$(4.14) \quad Q_r = \sum_i \sum_j n_{ij} y_{ij}^2 - \frac{1}{k}\sum_j B_j^2.$$

From (4.13) and (4.14) we obtain

$$Q_r - Q_a = \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij}\left[\hat{v}_i - \frac{1}{k}\sum_{i'=1}^{r} n_{i'j}\hat{v}_{i'}\right]^2.$$

Let $S_j = \sum_{i'=1}^{r} n_{i'j}\hat{v}_{i'}$. Then

$$Q_r - Q_a = \sum_i \sum_j n_{ij}\left(v_i - \frac{1}{k}S_j\right)^2 = r\sum_i \hat{v}_i^2 - \frac{2}{k}\sum_i \sum_j n_{ij}\hat{v}_i S_j + \frac{k}{k^2}\sum_j S_j^2$$

$$= r\sum_i \hat{v}_i^2 - \frac{2}{k}\sum_j S_j^2 + \frac{1}{k}\sum_j S_j^2$$

$$= r\sum_i \hat{v}_i^2 - \frac{1}{k}\sum_j S_j^2 .$$

But,

$$\sum_{j=1}^{b} S_j^2 = \sum_{i=1}^{r}\sum_{i'=1}^{r}\sum_{j=1}^{b} n_{i'j}n_{ij}\hat{v}_{i'}\hat{v}_i = \sum_{i=1}^{r}\sum_{i'=1}^{r}\left[\lambda + \delta_{ii'}(r-\lambda)\right]\hat{v}_{i'}\hat{v}_i$$

$$= (r-\lambda)\sum_{i=1}^{r}\hat{v}_i^2 ,$$

since the method for minimizing Q is equivalent to the method of Lagrange multipliers and hence the $\hat{v}_i$'s satisfy the condition $\sum_i v_i = o$. Thus

$$Q_r - Q_a = \frac{rk-r+\lambda}{k}\sum_{i=1}^{r}\hat{v}_i^2 \tag{4.15}$$

$$= \frac{\lambda v}{k}\sum_{i=1}^{r}\hat{v}_i^2 .$$

Also from (4.13)

$$Q_a = \sum_{i=1}^{r}\sum_{j=1}^{b} n_{ij}y_{ij}^2 - \frac{\lambda v}{k}\sum_{i=1}^{r}\hat{v}_i^2 - \frac{1}{k}\sum_{j=1}^{b} B_j^2 . \tag{4.16}$$

By (4.10)

$$\frac{\lambda v}{k}\sum_{i=1}^{r} v_i^2 = \frac{1}{\lambda k v}\sum_{i=1}^{r}(kV_i - T_i)^2$$

which is the best form for computing this term of Q_a.

Consider the set of bk expressions

$$E(y_{ij}) = \sum_{i'=1}^{r}\delta_{ii'}v_{i'} + \sum_{j'=1}^{b}\delta_{jj'}b_{j'} + \mu .$$

Denote the column vector of the coefficients of v_i by ν_i, the column vector corresponding to b_j by β_j, and the column vector corresponding to μ by I. Every element of I will be unity. To determine the rank of Q_a we need to know the rank of the matrix A, corresponding to the expressions

$$E(y_{ij}) = \sum_{i'=1}^{v-1} (\delta_{ii'} - \delta_{iv}) v_{i'} + \sum_{j'=1}^{b-1} (\delta_{jj'} - \delta_{jb}) b_{j'} + \mu .$$

In terms of the above notation we may write

$$A = (\nu_1 - \nu_v, \nu_2 - \nu_v, \ldots, \nu_{v-1} - \nu_v, \beta_1 - \beta_b, \beta_2 - \beta_b, \ldots, \beta_{b-1} - \beta_b, I)$$

In order to find the rank of A, we shall first determine the rank of the matrix

$$B = (\nu_1, \nu_2, \ldots, \nu_v, \beta_1, \ldots, \beta_b)$$

Let η be the observational vector whose elements are the y_{ij}'s arranged in the same order as the corresponding rows in A. Then

$\eta \cdot \nu_i = V_i$ = the total yield of the ith variety,

and

$\eta \cdot \beta_j = B_j$ = the total yield of the jth variety.

Since B_j and $B_{j'}$, $j' \neq j$, are the sums of different observations,

$$\operatorname{cov}(B_j, B_{j'}) = \sigma^2 (\beta_j \cdot \beta_{j'}) = 0.$$

Thus β_j is orthogonal to $\beta_{j'}$, $j' \neq j$, and hence the set of vectors $\beta_1, \ldots, \beta_b$ are linearly independent.

Consider the expression

$$Q_i = \frac{\lambda v}{k} \hat{v}_i = V_i - \frac{T_i}{k} = V_i - \frac{1}{k} \sum_j n_{ij} B_j$$

$$= \eta \cdot (\nu_i - \frac{1}{k} \sum_{j'} n_{ij'} \beta_{j'}) = \eta \cdot \gamma_i \text{ , say.}$$

The matrix

$$C = (\gamma_1, \gamma_2, \ldots, \gamma_v, \beta_1, \beta_2, \ldots, \beta_b)$$

has the same rank as the matrix B. We now compute

$$\operatorname{cov}(Q_i, B_j) = E(Q_i, B_j) - E(Q_i) E(B_j). \tag{4.17}$$

We have

$$E(Q_i,B_j) = E(V_i,B_j) - \frac{1}{k}\sum_{j'=1}^{b} n_{ij'} E(B_{j'},B_j).$$

If variety occurs in block j, then V_i and B_j have one observation in common, and

$$E(V_i,B_j) = \mathrm{cov}(V_i,B_j) + E(V_i)E(B_j)$$

$$= \sigma^2 + E(V_i)E(B_j).$$

If variety i does not occur in block j, then V_i and B_j have no observation, and

$$E(V_i,B_j) = E(V_i)E(B_j).$$

These two results may be combined into a single formula given by

$$E(V_i,B_j) = n_{ij}\sigma^2 + E(V_i)E(B_j).$$

In the same way it may be shown that

$$E(B_j,B_{j'}) = \delta_{jj'}k\sigma^2 + E(B_j)E(B_{j'}).$$

Hence

$$E(Q_i,B_j) = n_{ij}\sigma^2 + E(V_i)E(B_j) - \frac{1}{k}\sum_{j'=1}^{b} n_{ij'}\left[\delta_{jj'}k\sigma^2 + E(B_j)E(B_{j'})\right]$$

$$= n_{ij}\sigma^2 + E(V_i)E(B_j) - n_{ij}\sigma^2 - \frac{E(B_j)}{k}\sum_{j'=1}^{b} n_{ij'}E(B_{j'})$$

$$= \left[E(V_i) - \frac{1}{k}\sum n_{ij'}E(B_{j'})\right]E(B_j)$$

$$= E(Q_i)E(B_j).$$

Thus, from (4.17), $\mathrm{cov}(Q_i,B_j) = 0$. Hence γ_i is orthogonal to β_j for all values of i and j. It follows that

$$\left(\nu_i - \frac{1}{k}\sum_{j'} n_{ij'}\beta_{j'}\right)\cdot\beta_j = 0,$$

that is,

$$\nu_i\cdot\beta_j - \frac{1}{k}\sum_{j'} n_{ij'}(\beta_j\cdot\beta_{j'}) = \nu_i\cdot\beta_j - \frac{n_{ij}}{k}\beta_j^2$$

$$= \nu_i\cdot\beta_j - n_{ij} = 0.$$

Hence $\gamma_i \cdot \beta_j = n_{ij}$. By means of the methods used earlier it can be shown that

$$\operatorname{cov}(V_i, V_{i'}) = \delta_{ii'} r \sigma^2 = (\gamma_i \cdot \gamma_{i'})\sigma^2$$

so that $\gamma_i \cdot \gamma_{i'} = \delta_{ii'} r$.

Next, we compute the Gram matrix, G, of the matrix

$$D = (\gamma_1, \ldots \gamma_v).$$

We have

$$G = (\gamma_i \cdot \gamma_{i'})$$

where G is a square matrix of order v. Also

$$\begin{aligned}
\gamma_i \cdot \gamma_{i'} &= \left(\gamma_i - \frac{1}{k}\sum_{j'} n_{ij'}\beta_{j'}\right) \cdot \left(\gamma_{i'} - \frac{1}{k}\sum_{j} n_{i'j}\beta_j\right) \\
&= \delta_{ii'} r - \frac{1}{k}\sum_{j} n_{i'j} n_{ij} - \frac{1}{k}\sum_{j'} n_{ij'} n_{i'j'} + \frac{1}{k^2}\sum_{j'}\sum_{j} n_{ij'} n_{i'j} (\beta_j \cdot \beta_{j'}) \\
&= \delta_{ii'} r - \frac{1}{k}\left[\lambda + \delta_{ii'}(r - \lambda)\right] \\
&= -\frac{\lambda}{k}, \text{ if } i \neq i', \\
&= \frac{r(k-1)}{k}, \text{ if } i = i'.
\end{aligned}$$

Thus

$$G = \begin{pmatrix} \frac{r(k-1)}{k} & -\frac{\lambda}{k} & \cdots & -\frac{\lambda}{k} \\ -\frac{\lambda}{k} & \frac{r(k-1)}{k} & \cdots & -\frac{\lambda}{k} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ -\frac{\lambda}{k} & -\frac{\lambda}{k} & \cdots & \frac{r(k-1)}{k} \end{pmatrix}.$$

From previous work $|G| = \left[\frac{r(k-1)}{k} + \frac{\lambda}{r}\right]^{v-1}\left[-(v-1)\frac{\lambda}{k} + \frac{r(k-1)}{k}\right] = 0$ since $r(k-1) = \lambda(v-1)$. The value of the determinant obtained by deleting the first row and first column of $|G|$ is

$$\left[\frac{rk - r+\lambda}{k}\right]^{v-2}\left[-\frac{(v-2)\lambda}{k} + \frac{r(k-1)}{k}\right]$$

$$= (\lambda v/k)^{v-2}\left[\frac{\lambda}{k} - \frac{(v-1)\lambda}{k} + \frac{r(k-1)}{k}\right] = \frac{1}{v}\left(\frac{v\lambda}{k}\right)^{v-1} \neq 0.$$

Thus the matrix G, and hence D, is of rank v - 1. Hence v - 1 of the vectors $\gamma_1, \ldots, \gamma_v$ are linearly independent and orthogonal to the β_j's. By Theorem 3.5, the matrix C and hence the matrix B is of rank v + b - 1.

Next note that

$$\sum_{i=1}^{v} \eta \cdot \gamma_i \equiv \sum_{i=1}^{v} Q_i \equiv \frac{\lambda v}{k} \sum_i \hat{v}_i \equiv 0,$$

and hence

$$0 = \sum_{i=1}^{v} \gamma_i = \sum_{i=1}^{v} \nu_i - \frac{1}{k}\sum_i \sum_j n_{ij}\beta_j = \sum_{i=1}^{v} \nu_i - \sum_j \beta_j$$

Thus any v + b - 1 column vectors from B are linearly independent.

We shall now prove that the matrix

$$(\nu_1 - \nu_v, \nu_2 - \nu_v, \ldots, \nu_{v-1} - \nu_v, \beta_1 - \beta_b, \beta_2 - \beta_b, \ldots, \beta_{b-1} - \beta_b)$$

is of rank v + b - 2. Consider the equation

$$\sum_{i=1}^{v-1} c_i(\nu_i - \nu_v) + \sum_{j=1}^{b-1}(\beta_j - \beta_b) = 0.$$

This equation may be written in the form

$$\sum_{i=1}^{v-1} c_i(\nu_i - \nu_v) + \sum_{j=1}^{b-1} d_j\beta_j - \beta_b \sum_{j'=1}^{b-1} d_{j'}$$

$$= \sum_{i=1}^{v-1} c_i(\nu_i - \nu_v) + \sum_{j=1}^{b-1} d_j\beta_j - \left(\sum_{i=1}^{v} \nu_i - \sum_{j=1}^{b-1}\beta_j\right)\sum_{j'=1}^{b-1} d_{j'}$$

$$= \sum_{i=1}^{v-1}\left(c_i - \sum_{j'=1}^{b-1} d_{j'}\right)\nu_i + \sum_{j=1}^{b-1}\left(d_j + \sum_{j'=1}^{b-1} d_{j'}\right)\beta_j - \left(\sum_{i=1}^{v-1} c_i + \sum_{j'=1}^{b-1} d_{j'}\right)\nu_v = 0.$$

Since $\nu_1, \ldots, \nu_v, \beta_1, \ldots, \beta_{b-1}$ are linearly independent we have

$$d_j + \sum_{j'=1}^{b-1} d_{j'} = 0, \quad j = 1, \ldots, b-1;$$

$$c_i - \sum_{j'=1}^{b-1} d_{j'} = 0, \quad i = 1, \ldots, v-1;$$

$$\sum_{i=1}^{v-1} c_i + \sum_{j'=1}^{b-1} d_{j'} = 0.$$

The $(b-1)$th order determinant of the coefficients of the first set of equations is

$$\begin{vmatrix} 2 & 1 & 1 & \ldots & 1 \\ 1 & 2 & 1 & \ldots & 1 \\ \cdot & & & & \\ \cdot & \cdot & & \cdot & 1 \\ \cdot & \cdot & & \cdot & \\ 1 & \ldots & 1 & & 2 \end{vmatrix} = (2-1)^{b-2}\left[(b-2)+2\right] \neq 0.$$

Hence $d_1 = d_2 = \ldots = d_{b-1} = 0$. Then, from the second set of equations, $c_1 = c_2 = \ldots = c_{v-1} = 0$. Hence the last equation is also satisfied. Thus

$$\nu_1 - \nu_v, \ldots, \nu_{v-1} - \nu_v, \beta_1 - \beta_b, \ldots, \beta_{b-1} - \beta_b$$

are linearly independent vectors.

Finally,

$$(\nu_{i'} - \nu_v).I = \sum_i \sum_j n_{ij}(\delta_{ii'} - \delta_{iv}) = r \sum_i (\delta_{ii'} - \delta_{iv}) = 0,$$

and

$$(\beta_{j'} - \beta_b).I = \sum_i \sum_j n_{ij}(\delta_{jj'} - \delta_{jb}) = k \sum_j (\delta_{jj'} - \delta_{jb}) = 0.$$

Thus, by Theorem 3.5, the set of $v + b - 1$ vectors

$$\nu_1 - \nu_v, \ldots, \nu_{v-1} - \nu_v; \beta_1 - \beta_b, \ldots, \beta_{b-1} - \beta_b, I$$

are linearly independent. Hence $r(A) = v + b - 1$ and thus $r(Q_a) = vr - v - b + 1$.

It remains to determine the rank of $Q_r - Q_a$. Since $\sum \hat{v}_i = 0$, it follows that

$$r\left[\frac{\lambda v}{k}\sum_i \hat{v}_i^2\right] \leq v - 1.$$

Since $\sum_j (\frac{B_j}{k} - y) = kby/k - by = 0$, we have

$$r\left[k\sum_j (\frac{B_j}{k} - y)^2\right] \leq b - 1.$$

The rank of kby^2 is 1.

From (4.12) and Theorem 3.5 we have

$$rv = r\left[\sum_i\sum_j n_{ij}y_{ij}^2\right] \leq r[Q_a] + r\left[\frac{\lambda v}{k}\sum_i \hat{v}_i^2\right] + r\left[k\sum_j (\frac{B_j}{k} - y)^2\right] + r[kby^2]$$

$$= rv - v - b + 1 + v - 1 + b - 1 + 1 = rv.$$

Hence the equality signs must hold throughout. Thus the quadratic form $Q_r - Q_a$ must have rank $v - 1$.

To test the hypothesis $v_i = 0$, $i = 1,\ldots,v$, we use the statistic

$$F = \frac{rv - v - b + 1}{v - 1} \cdot \frac{\frac{\lambda v}{k}\sum_i \hat{v}_i^2}{\sum_i\sum_j n_{ij}y_{ij}^2 - \frac{\lambda v}{k}\sum_i \hat{v}_i^2 - (1/k)\sum_j B_j^2}$$

$$\frac{rv - v - b + 1}{v - 1} \cdot \frac{\sum_i (kV_i - T_i)^2}{\lambda kv\sum_i\sum_j n_{ij}y_{ij}^2 - \sum_i (kV_i - T_i)^2 - \lambda v\sum_j B_j^2}.$$

To test the hypotheses $v_i = v_j$ we use the Corollary to Theorem 3.3. Notice that Q_a remains unchanged. From the corollary we see that $v_i - v_j$ corresponds to β_i^*. The rank of the matrix of coefficients (1,-1) is 1. Since $\hat{v}_i$ and $\hat{v}_j$ are the estimates of v_i and v_j which minimize Q_a we have

$$b_1^* = \hat{v}_i - \hat{v}_j .$$

Also, since $i = j = 1$, the matrix of coefficients (c_{ij}) of $Q_r - Q_a$ is

$$c_{11} = \frac{\sigma^2}{\sigma^2_{b_1^*}}$$

Now

$$\sigma^2_{b_1^*} = \sigma^2_{\hat{v}_i - \hat{v}_j} = E\left[(\hat{v}_i - \hat{v}_j) - E(\hat{v}_i - \hat{v}_j)\right]^2$$

$$= E\left[(\hat{v}_i - E(\hat{v}_i)) - (\hat{v}_j - E(\hat{v}_j))\right]^2$$

$$= \sigma^2_{\hat{v}_i} + \sigma^2_{\hat{v}_j} - 2\sigma_{\hat{v}_i \hat{v}_j} .$$

From (4.10) we have

$$\hat{v}_i = \frac{1}{\lambda v}\left[(k-1)V_i - (T_i - V_i)\right]$$

Since $T_i = \sum_j n_{ij} B_j$ and $B_j = \sum_{i'} n_{i'j} y_{i'j}$, $V_i = \sum_j n_{ij} y_{ij}$,

we have

$$T_i - V_i = \sum_{j=1}^{b}\left(\sum_{i'=1}^{a} n_{ij} n_{i'j} y_{i'j} - n_{ij}^2 y_{ij}\right)$$

$$= \sum_{j=1}^{b} \sum_{\substack{i'=1 \\ i' \neq i}}^{a} n_{ij} n_{i'j} y_{i'j} .$$

Thus V_i and $T_i - V_i$ have no observations in common and hence $(k-1)V_i$ and $T_i - V_i$ are independently distributed. Therefore

$$\sigma^2_{\hat{v}_i} = \frac{1}{\lambda^2 v^2}\left[(k-1)^2 \sigma^2_{V_i} + \sigma^2_{T_i - V_i}\right] \quad [1]$$

Also

$$\sigma^2_{V_i} = \sigma^2 \sum_{j=1}^{b} n_{ij}^2 = \sigma^2 \sum_{j=1}^{b} n_{ij} = r\sigma^2$$

---

[1] Wilks, p. 35.

and

$$\sigma^2_{T_i - V_i} = \sigma^2 \sum_{\substack{i'=1 \\ i' \neq i}}^{v} \sum_{j=1}^{b} n_{i'j}^2 n_{ij}^2 = \sigma^2 \sum_{i'=1}^{v} \left[\lambda + \delta_{ii'}(r - \lambda) \right]$$

$$= \lambda(v - 1)\sigma^2 = r(k - 1)\sigma^2.$$

Therefore

$$\sigma^2_{\hat{v}_i} = \frac{1}{\lambda^2 v^2}\left[(k - 1)^2 r\sigma^2 + r(k - 1)\sigma^2\right]$$

$$= \frac{rk(k - 1)\sigma^2}{\lambda^2 v^2} = \frac{k\lambda(v - 1)\sigma^2}{\lambda^2 v^2} = \frac{k(v - 1)\sigma^2}{\lambda v^2}.$$

Since the last expression is independent of i we also have

$$\sigma^2_{\hat{v}_j} = \frac{k(v - 1)\sigma^2}{\lambda v^2}.$$

From Corollary 3.3

$$Q_r - Q_a = c_{11} b_1^{*2}$$

$$= \frac{\sigma^2}{\lambda^2 v^2 \sigma^2_{\hat{v}_i - \hat{v}_j}} \left[k(V_i - V_j) - (T_i - T_j)\right]^2$$

$$= \frac{1}{2\lambda k v} \left[k(V_i - V_j) - (T_i - T_j)\right]^2.$$

The number of degrees of freedom of $Q_r - Q_a$ is 1. Hence, to test the hypothesis $v_i = v_j$ we use the statistic

$$F_1 = \frac{rv - v - b + 1}{2k\lambda v} \cdot \frac{\left[k(V_i - V_j) - (T_i - T_j)\right]^2}{Q_a}$$

where F_1 has the F distribution with 1 and $rv - v - b + 1$ degrees of freedom.

Each variety appears r times. Suppose we use r blocks

with v plots so that every variety appears in every block in a two-way classification design. For this design let

$$\sigma^2_{\hat{v}_i} = \sigma^2/h.$$

For the incomplete balanced block design let

$$\sigma^2_{\hat{v}_i} = \sigma^2/c_i.$$

Definition: The efficiency factor of an incomplete balanced block design with respect to the estimate $\hat{v}_i$, as compared with the two-way classification design, is

$$e = (\sigma^2/h)/(\sigma^2/c_i) = c_i/h.$$

Note that if the incomplete balanced block design has a smaller variance for $\hat{v}_i$, then $e > 1$. The efficiency factors with respect to varietal differences are defined similarly. Clearly if there is a choice between two designs, one of which is more efficient than the other while both justify the assumption (4.3), then the experimenter will choose the more efficient design.

In an incomplete balanced block design we already know that

$$\sigma^2_{\hat{v}_i} = \frac{k(v-1)}{\lambda v^2}\sigma^2.$$

In a two-way classification design, $k = v$, $\lambda = r$. Hence for the latter design

$$\sigma^2_{\hat{v}_i} = \frac{v(v-1)}{r v^2}\sigma^2 = \frac{v-1}{rv}\sigma^2.$$

Thus the efficiency factor with respect to the estimate $\hat{v}_i$ is

$$e = \frac{v-1}{rv} \cdot \frac{v^2\lambda}{k(v-1)} = \frac{\lambda v}{rk}.$$

For an incomplete balanced block design

$$\sigma^2_{\hat{v}_i-\hat{v}_j} = \frac{2k}{\lambda v}\sigma^2.$$

For a two-way classification design

$$\sigma^2_{\hat{v}_i-\hat{v}_j} = \frac{2}{r}\sigma^2.$$

Hence the efficiency factor with respect to the estimate v_i-v_j is

$$e = \frac{2\lambda v}{r2k} = \frac{\lambda v}{rk},$$

as before.

For example, in the design $(v,b,r,k,\lambda) = (16,24,9,6,3)$, $(8,14,7,4,3)$, $(11,11,5,5,2)$, and $(21,21,5,5,1)$, the value of the efficiency factors with respect to the estimates $\hat{v}_i$ and $\hat{v}_i-\hat{v}_j$ are 8/9, 6/7, 22/25, and 21/25 respectively.

The loss of efficiency will, in general, be more than offset by the reduction in the error variance per plot resulting from the use of smaller, more homogeneous, blocks.

BIBLIOGRAPHY

Attridge, R.F., Multiple Classification Designs. McMaster University, 1952.

Birkhoff, G., and MacLane S., A Survey of Modern Algebra. New York: MacMillan, 1948.

Dickson, L.E., First Course in the Theory of Equations. New York: Wiley, 1922.

Kempthorne, O., The Design and Analysis of Experiments. New York: Wiley, 1952.

MacDuffee. C.C., Introduction to Abstract Algebra. New York: McGraw-Hill, 1939.

Mann, H.B., Analysis and Design of Experiments. New York: Dover, 1949.

Mood, A.M., Introduction to the Theory of Statistics. New York: McGraw-Hill, 1950.

Schwerdtfeger, H., Introduction to Linear Algebra and the Theory of Matrices. Groningen, Holland: P. Noordhoff N.V., 1950.

Uspensky, J.V., and Heaslet, M.H., Elementary Number Theory. New York: McGraw-Hill, 1939.

Wilks, S.S., Mathematical Statistics. Princeton: Princeton University Press, 1950.