Summer Course (advanced) for Statisticians

May–June 1961

LECTURE NOTES No.—1

COMBINATORIAL PROBLEMS

by S. S. Shrikhande, Professor of Statistics, Banaras Hindu University

RESEARCH AND TRAINING SCHOOL
INDIAN STATISTICAL INSTITUTE
203 BARRACKPORE TRUNK ROAD
CALCUTTA-35

COMBINATORIAL PROBLEMS

by

S.S.Shrikhande

C O N T E N T S

Research and Training School
Indian Statistical Institute
203,Barrackpore Trunk Road,
Calcutta-35.

Lecture 1

A. Elementary Theory of Groups

Definition 1. A group G is a set of elements G(a, b, c,...) and a binary operation between any two elements a and b denoted by ab such that the following conditions are satisfied.

I. If a and b are elements of G, whether identical or distinct, then ab is also an element of G.

II. For any three elements a, b, c of G, (ab)c = a(bc).

III. The set G contains an element 1, called the identity, such that $a1 = 1a = a$ for every element a of G.

IV. For any a in G there exists an element denoted by a^{-1} such that $a\,a^{-1} = a^{-1}a = 1$.

These laws are redundant. We may replace III and IV by

III* There exists an element 1, such that $1a = a$ for every a in G.

and IV* For every a of G, there exists an element x such that $xa=1$.

We can show that these in turn imply III and IV. This is left as an exercise.

A group G is said to be finite or infinite according as the number of elements in it is finite/infinite. If G contains n elements, where n is finite, then n is called the order of the finite group G.

It is easy to establish the uniqueness of 1 and a^{-1}. An important consequence of the associative law is the generalised associative law which states that,

'All ways of bracketing an ordered sequence $a_1, a_2, \ldots, a_n$ to give it a value by calculating a succession of binary products yield the same result'

Examples. All nth roots of unity under multiplication, residue classes (mod. n) under addition form groups.

Definition 2. A subset H of a group G is called a subgroup if the following conditions hold:

S_1. If $h_1 \varepsilon H$, $h_2 \varepsilon H$, then $h_1 h_2 \varepsilon H$

S_2. If $h_1 \varepsilon H$, then $h_1^{-1} \varepsilon H$.

The set of all even integers form a subgroup of the set of all integers.

Definition 3. A one-to-one mapping $G \leftrightarrow H$ of the elements of a group G onto those of a group H is called an isomorphism, if whenever $g_1 \leftrightarrow h_1$ $g_2 \leftrightarrow h_2$, then $g_1 g_2 \leftrightarrow h_1 h_2$.

Example. Consider the following permutations.

	G_1				G_2					
	(1	2	3)		(1	2	3	4	5	6)
X_1 =	(1	2	3)	Y_1 =	(1	2	3	4	5	6)
Y_2 =	(2	3	1)	Y_2 =	(2	3	1	6	4	5)
X_3 =	(3	1	2)	Y_3 =	(3	1	2	5	6	4)
X_4 =	(1	3	2)	Y_4 =	(4	5	6	1	2	3)
X_5 =	(3	2	1)	Y_5 =	(5	6	4	3	1	2)
X_6 =	(2	1	3)	Y_6 =	(6	4	5	2	3	1)

It is easy to verify that G_1 and G_2 are groups which are isomorphic.

Definition 4. A mapping $G \to H$ of the elements of a group G onto those of a group H is called a homomorphism if whenever $g_1 \to h_1$, $g_2 \to h_2$, then $g_1 g_2 \to h_1 h_2$.

A homomorphism takes unit into unit and inverses into inverses. In the above example $X_1, X_2, X_3 \to 1$, $X_4, X_5, X_6 \to -1$ is a homomorphism.

In what follows we shall consider abelian groups satisfying

V. $ab = ba$ for all a and b in G.

Cosets.

Given a group G and a subgroup H, the set of all elements hx, $h \in H$, $x \in G$, x fixed is called a coset denoted by Hx.

Theorem 1. Two cosets of H in G are either identical or disjoint coset of H contains the same cardinal number of elements as H.

Proof. If Hx and Hy have nothing in common, there is nothing to prove. Hence suppose $z \in Hx$ and $z \in Hy$. Then $z = h_1x = h_2y$. Hence $x = h_1^{-1} h_2 y$ and $hx = hh_1^{-1} h_2 y = h'y$ hence $Hx \subseteq Hy$. Similarly $Hy \subseteq Hx$. Hence $Hx = Hy$. Then correspondence $h \leftrightarrow hx$ shows that H and Hx contain the same cardinal number of elements. We can then write

$$G = H + Hx_2 + \cdots + Hx_r .$$

The cardinal number r is called the index of H in G. The order of G is the cardinal number of elements in G.

Theorem 2. The order of G is the product of the order of a subgroup H and the index of H in G.

Cor. For any $a \in G$, $a^p = 1$ if p is the order of G

(Consider the cyclic subgroup generated by a.)

Direct products. A and B are two groups. Form the ordered pair (a, b), $a \in A$, $b \in B$; then the ordered pairs (a, b) form a group if we define

$$(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$$

Moreover $(a, b) \leftrightarrow (b, a)$ shows that A x B and B x A are isomorphic. The correspondence $a \leftrightarrow (a, 1)$ is an isomorphism of A with the set of elements in A x B with second component identity. Similarly for B. We can identify A and B with these subgroups of A x B and say that G = A x B is the direct product of its subgroups A and B. Since (a, 1) (1, b)=(a, b)= (1 , b)(a, 1) it follows that in A x B every element of A commutes with every element of B i.e. ab = ba for $a \in A$, $b \in B$.

Examples. Let B_n be the group of n-place binary sequences under the operation of addition mod.2. It is the direct product A x A x ... x A (n times) where A is the additive group with symbols 0 and 1 such that 0 + 0 = 1 + 1 = 0, 0 + 1 = 1 + 0 = 1. The order of the group is 2^n. It is isomorphic with the group C_n generated by n commutating elements of order two, say, $a_1, a_2, \ldots, a_n$. Here $a_i a_j = a_j a_i$ and $a_i^2 = I$, $i,j = 1,2,\ldots,n$ and I is the identity of the group. For example C_3 is the group of elements I, a_1, a_2, a_3, a_1a_2, a_1a_3, a_2a_3, $a_1a_2a_3$. The group C_n is isomorphic with the n fold direct product of C_1 with itself. A convenient way of writing down the above elements is I, 1, 2, 3, 12, 13, 23, 123. In this notation (1 2)(2 3 4) = (1 3 4). In general the product of a number of factors in this notation is the symbol containing only those integers which occur odd number of times in the factors.

The isomorphism between B_n and C_n can be established in many ways. The most convenient way, perhaps, is to associate with the element $i_1, i_2, \ldots, i_k$ of C_n, the element of B_n which has one, in place $i_1, i_2, \ldots, i_k$ and zero elsewhere. For example the element 124 of C_4 can be associated with (1101) of B_4.

An element T of C_n is said to be dependent upon the set of elements $T_1, T_2, \ldots, T_j$ of C_n if T can be expressed as a product of some elements of the set $T_1, T_2, \ldots, T_j$; otherwise T is said to be independent of the set. A set is said to be independent if no member is dependent upon the rest. For example in C_4 the set 1, 2, 3, 4 form an independent set. Any set of n independent elements of C_n can be taken as generators of C_n, for the relation

$$\binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n} = 2^n - 1$$

gives 2^n-1 elements of C_n different from I and T is the product of any element with itself.

Any k independent elements of C_n serve as generators of a subgroup of order 2^k. The subgroup generated is clearly isomorphic with C_k

The number of ways in which k independent elements can be chosen from 2^n elements of C_n is

$$F(n,k) = (2^n - 2^0)(2^n - 2^1)(2^n - 2^2)\ldots(2^n - 2^{k-1}).$$

For the first element can be chosen in 2^n-1 ways (the identity can not be included in a non-trivial set of independent elements) and the second in 2^n-2 ways. They determine a subgroup of order 2^2. The third element can be chosen in the remaining 2^n-2^2 ways. The 3 chosen elements form a subgroup of order 2^3. Hence generalising we get the required result.

Each set of k independent elements determine a subgroup of order 2^k. F(n, k), however, is not the number of different subgroups of C_n of order 2^k. Since each subgroup of order 2^k can obviously be determined by choosing k independent elements of that group, which can be done in F(k, k) ways (the subgroup being isomorphic with C_k), the total number of distinct subgroups is $F(n, k)/F(k, k) = N(n, k)$. A simple calculation shows that $N(n, k) = N(n, n-k)$.

In B_n, regarding each element as a vector over the field GF(2); it is obvious that a set of k elements of B_n are independent if and only if the matrix of the corresponding vectors is nonsingular in GF(2). If $x_1, x_2, \ldots, x_k$ are k independent elements of B_n, the subgroup of B_n generated by these elements is the set of elements $\lambda_1 x_1 + \lambda_2 x_2 + \ldots + \lambda_k x_k$ where $\lambda_i = 0$ or 1.

B. Elementary theory of Galois Fields

1. A set of elements a, b, c ... is said to form a field F when there exist two laws of composition, i.e. addition (denoted by +) and multiplication (denoted by x or a dot), such that the following axioms are satisfied.

Closure laws

For any a, b ε F there exists a unique element c ε F such that $a+b = c$.

For any a, b, ε F, there exists a unique element d ε F such that ab = d.

Associative laws

$$(a+b) + c = a + (b+c)$$
$$(ab)c = a(bc)$$

Commutative laws

$$b+a = a+b$$
$$ba = ab$$

Zero and Unit

0 exists such that $a + 0 = 0 + a = a$

1 exists such that $a.1 = 1.a = a$

for all $a \varepsilon F$.

Negatives and Inverses

For every a, -a exists such that $(-a) + (a) = a+(-a) = 0$

For every $a \neq 0$, a^{-1} exists such that $a(a^{-1}) = (a^{-1})(a) = 1$.

Distributive law

$$a(b + c) = ab + ac$$
$$(b + c)a = ba + ca$$

It follows easily that 0 and 1 are unique and that $a.0 = 0$ for any a in F and that $1 \neq 0$.

It can be easily satisfied that the above axioms are satisfied by the system of all rational numbers, all real numbers, all complex numbers which are examples of fields containing an infinite number of elements. We are interested here in fields containing a finite number of elements. Such fields are called Galois fields.

2. The simplest example of a Galois field is provided by the field of residue classes modulo p, p being any prime positive integer. Let all integers congruent to a mod p be considered to form a class denoted by (a). Then there exist only p different classes (0), (1), ..., (p-1). The addition and multiplication of these classes is defined by

$$(a) + (b) = (a + b)$$
$$(a)(b) = (ab)$$

It can be verified that all the axioms of a field are satisfied. This field is usually denoted by GF_p, obviously any integer of the class (a) will give rise to same class as (a). There is only one non-negative integer less than p representative of (a). This may be called the standard representative of (a).

3. The concept of a polynomial in ordinary algebra can be extended to any field. The expressions of the type

$$f(x) = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$$

with coefficients in a field F constitute the set of polynomials belonging to a commutative ring $F[x]$, addition and multiplication being defined in the usual manner. For polynomials belonging to $GF_p[x]$, the coefficients are residue classes mod p.

A polynomial $f(x)$ of $F[x]$ is called irreducible, when it is impossible to find polynomials $\phi(x)$ and $\alpha(x)$ of $F[x]$ of degree m and n, $m \geq 1$, $n \geq 1$, such that

$$f(x) = \phi(x)\ \alpha(x).$$

If however $\phi(x)$ and $\alpha(x)$ can be found as above then $f(x)$ is said to be reducible and $\phi(x)$ and $\alpha(x)$ are called factors of $f(x)$.

Let $f(x)$ be an irreducible polynomial of $F[x]$. Two polynomials $\phi_1(x)$ and $\phi_2(x)$ are said to be congruent modulo $f(x)$ if $\phi_1(x) - \phi_2(x)$ has a factor $f(x)$ and we write $\phi_1(x) \equiv \phi_2(x) \pmod{f(x)}$. The class of polynomials congruent to $\phi(x)$ may be written as $[\phi(x)]$ and we define

$$[\phi(x)] + [\alpha(x)] = [\phi(x) + \alpha(x)]$$
$$[\phi(x)]\ \ [\alpha(x)] = [\phi(x)\ \ \alpha(x)]$$

It can be shown that these classes form a field. The polynomial $\phi(x)$ is said to be a representative of the class $[\phi(x)]$. If $f(x)$ is of degree n, there is only one polynomial of degree less than n, which represents $[\phi(x)]$. This may be called the standard representative of $[\phi(x)]$.

4. It is easy to prove the following facts about a finite field.

(i) The number of elements in a finite field is the power of a prime For each prime power p^r there is a finite field $GF(p^r)$ with p^r elements and it is unique to within isomorphism.

(ii) Each element of x satisfies the relation $x^{p^r} = x$. The multiplicative group $F^*(p^r)$ of the p^r-1 elements of $GF(p^r)$, excluding zero is cyclic. A generator of this group is called a primitive element.

(iii) $GF(p^r)$ may be represented as the residue classes of polynomials $P(x)$ with coefficients in the field GF_p, modulo a polynomial $f(x)$ irreducible of degree r over GF_p.

Because of isomorphism between any two Galois fields with the same number of elements it is sufficient to write down the elements of any Galois field with a given number of elements together with the addition and multiplication table.

Examples of finite fields.

(i) The polynomial $x^2 + x + 1$ is irreducible over GF_2. Hence the elements of $GF(2^2)$ are 0, 1, x, x + 1 with the following addition and multiplication tables

Addition

	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

Multiplication

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

From the multiplication table we have $x = x$, $x^2 = x+1$, $x^3 = 1$, thus x is a primitive element of the field $GF(2^2)$ constructed above.

(ii) Show that $x^3 + x + 1$, $x^3 + x^2 + 1$, $x^4 + x + 1$, are irreducible GF_2 and that $x^3 - x + 1$, $x^3 - x + 2$ are irreducible over GF_3. Form the corresponding Galois fields.

In the construction of $GF(p^r)$ it is convenient to choose the irreducible polynomial of degree r over GF_p in such a way that x is a primitive element of the corresponding finite field. This may be done as follows.

Consider the equation $x^{p^r-1} = 1$, of ordinary algebra and obtain in the usual manner the cyclotomic equation i.e. the equation, which has for its roots, all the primitive roots of this equation. It is well known that the degree of this equation will be $m = \phi(p^r-1)$ where $\phi(k)$ denotes the number of positive integers less than k and relatively prime to it. Suppose this equation is

$$x^m + a_{m-1} x^{m-1} + \ldots + a_o = 0$$

where $a_{m-1}, \ldots, a_o$ are integers. Replacing a_i by its residue class (a_i) modulo p, we get the polynomial

$$x^m + (a_{m-1}) x^{m-1} + \ldots + (a_o)$$

of GF_p, which may be called the cyclotomic polynomial of order m of $GF_p[x]$. Let $f(x)$ be an irreducible factor of this equation. Consider the class of all polynomials of $GF_p[x]$ congruent modulo $f(x)$. Then these classes form a Galois field with p^r elements, the addition and multiplication being carried out in the usual manner modulo $f(x)$. The degree of $f(x)$ is always r. The polynomial $f(x)$ obtained above may be called the minimum function.

Instead of these classes, we may write down their standard representation, replacing each class by the unique polynomial of degree less than r with coefficients which are residues modulo p, provided we remember this fact at the time of forming sums and products. Then each element of the Galois field assumes the standard form

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

where $a_0, a_1 \ldots, a_{r-1}$ are integers taking any value between 0 and p-1.

Discussion of special cases.

(i) Galois field $GF(2^2)$.

Every element other than 0 satisfies $x^3 - 1 = 0$. The ordinary cyclotomic polynomial is $x^2 + x + 1$ which may be regarded also as the cyclotomic polynomial of $GF_2[x]$. Since $x^2 + x + 1$ is irreducible over GF_2, the minimum function is $f(x) = x^2 + x + 1$.

(ii) Galois field $GF(2^4)$.

Consider the equation $x^{15} - 1 = 0$. Since $x^m - 1 = 0$ with x in $GF(2^4)$ implies that m is a factor of 15, we omit those roots corresponding to m = 1,3 and 5, taking care that each such root is omitted only once. Hence we remove the factors x-1, $x^2 + x + 1$ and $x^4 + x^3 + x^2 + x + 1$ from $x^{15} - 1$ and get the cyclotomic polynomial in $GF_2[x]$ which is

$$x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$$

which is of degree $\phi(15) = 8$. It is easy to verify that this factors into two polynomials of degree 4. They are

$$x^4 + x^3 + 1 \qquad \text{and} \qquad x^4 + x + 1$$

each of which may be taken as the minimum function.

Write down the corresponding Galois fields and exhibit an isomorphism between them.

In a finite field all the four fundamental operations of ordinary arithmetic can be carried out. Hence all the concepts and results which depend only on these operations in the field of real numbers can be extended to a finite field. We can thus define vectors and matrices with elements in a finite field and also the rank of such a matrix. We can solve a set of linear equations with coefficients in a finite field with solutions in the field in an analogous manner.

Suggested reading

A. 1. Marshall Hall : The Theory of Groups (1959) MacMillan (New York).

2. Birkhoff and Mclane : Survey of modern Algebra.

3. Carmichael : Finite Groups.

B. 1. H. B. Mann : Design and analysis of experiments.

Lecture 2

Complete sets of mutually orthogonal Latin Squares

1. A Latin square of order v is an v x v array, the v^2 cells of which are occupied by v distinct symbols (which may be Latin or Greek letters or just plain integers) such that each symbol occurs once in every row and once in every column. For example, the square exhibited in Figure 1 is a Latin square of order 3

1	2	3
2	3	1
3	1	2

Figure 1

Two Latin squares of the same order are said to be orthogonal if, on superposition, each symbol of the first square occurs exactly once with each symbol of the second square. Two orthogonal Latin squares of order 4 are exhibited in Figure 2.

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

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

Figure 2

A set of Latin squares all of the same order is said to be a set of mutually orthogonal Latin squares (m.o. L.S.) if any two Latin squares of the set are orthogonal.

A Latin square is said to be in the standard form if the initial row contains the symbols in the natural order. Thus if the symbols are the integers 0, 1, 2, ..., v-1, the square is in the standard form if the initial row is 0, 1, 2, ..., v-1. A Latin square can always be brought in the standard form by renaming the symbols. If two Latin squares are orthogonal, the renaming can be done independently for each square without destroying the property of orthogonality. Thus in Figure 2,

by making the transformation

$$0 \longrightarrow 0,\quad 2 \longrightarrow 1,\quad 1 \longrightarrow 2,\quad 3 \longrightarrow 3$$

in the first square and the transformation

$$1 \longrightarrow 0,\quad 0 \longrightarrow 1,\quad 2 \longrightarrow 2,\quad 3 \longrightarrow 3$$

in the second square, we can exhibit the Latin squares in the standard form.

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

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

Figure 3

Given any Latin square of order v, number the rows (columns) of the square as 0,1,2,... v-1. The cell in i-th row and j-th column will be called the cell (i, j).

2. Denote by N(v) the maximum number of Latin squares of order v such that any two of them are orthogonal. We have

Theorem 1 : For any positive integer v, $N(v) \leq v-1$.

Proof: Suppose that the maximum number of m.o.L.S. is n. Without loss of generality the set can be put in the standard form. Consider any two Latin squares of the set. The cell (0, j) accounts for the pair (j, j) on superposition. Hence in the cell (i, j), $i \neq 0$, each Latin square contains a symbol $\neq j$. Further the same symbol cannot occur in this cell in both the Latin squares, for the identical pairs are provided on superposion by the first row. Hence in the n Latin squares the symbols in cell (i, j) are all different from one another and also different from j. Since there are only v-1 symbols different from j we have $n \leq v-1$.

A set of v-1 m.o.L.S. of order v is said to be a complete set of m.o.L.S. of order v.

Theorem 2: Any set of v-2 m.o.L.S. of order v can be extended to a complete set of v-1 m.o.L.S.

Proof: Let the symbols of each Latin Square be the integers 0, 1, 2,... v-1. Without loss of generality take the set $L_1, L_2, \ldots, L_{v-2}$ of m.o.L.S. in the standard form. Form a new square L containing the initial row in the standard form and put in the cell (i, j) for $i \neq 0$, that integer different from j which does not occur in this cell in any L_k, k = 1, 2, ..., v-2. We show that L is a Latin square which is orthogonal to every L_k. Since the cells (i, j) of L, $L_1, \ldots, L_{v-2}$ contain all the integers different from j exactly once, it is obvious that the ith row of L, $L_1, \ldots, L_{v-2}$ contains all the integers exactly v-1 times. But the ith row of $L_1, \ldots, L_{v-2}$ contains all these integers exactly v-2 times. Hence L contains all the integers in the ith row exactly once. Similarly it can be shown that every column of L contains all the integers exactly once. Thus L is a Latin square. Now consider L_1 and take the cells in which 0 occurs omitting the cell in the initial row. In these cells of L, $L_2, \ldots, L_{v-2}$ all the symbols excepting 0 occur exactly v-2 times, whereas by orthogonality these cells of $L_2, \ldots, L_{v-2}$ contain these symbols exactly v-3 times. Hence in L all the symbols excepting 0 occur exactly once in these cells, since the pair (0, 0) is obtained from the initial rows of L_1 and L, it is obvious that on superposition of L on L_1, 0 of L_1 occurs with all other integers. Similar argument shows that all other ordered pairs occur exactly once. Hence L is orthogonal to L_1. Similarly it is orthogonal to all the other Latin squares.

We state without proof the following theorem (Shrinkhande) due to appear in the coming issue of Sankhyā.

Theorem 3: If $v \neq 4$, then any set of v-3 m.o.L.S. of order v can be uniquely extended to a complete set of v-1 m.o.L.S.

3. Construction of complete sets of m.o.L.S.

If v is a prime power, we can obtain a complete set of m.o.L.S. of order v. There is no known example of a complete set of order v when v is not a prime power, though the existence of such a set has been disproved for certain values of v which are not prime powers.

Theorem 4: If v is a prime power, $N(v) = v-1$.

Proof: Let $v = p^n$ where p is a prime. Consider the Galois field $GF(p^n)$ with elements $\alpha_0 = 0, \alpha_1 = 1, \alpha_2, \ldots, \alpha_{v-1}$. Take $v \times v$ square and put in the cell (i, j) $i, j = 0, 1, \ldots, v-1$ the symbol x determined by

$$\alpha_x = \alpha_u \cdot \alpha_i + \alpha_j$$

where α_u is a fixed non-zero element of $GF(p^n)$. For a fixed i it is obvious that as j varies over the set $0, 1, \ldots, v-1$, α_x varies over all the elements of $GF(p^n)$. Similarly for a fixed j, $\alpha_u \alpha_j$ varies over all the elements of $GF(p^n)$ and hence so does α_x. Thus the square array is a Latin square which we may denote by L_u. We thus get $v-1$ Latin squares $L_1, L_2, \ldots, L_{v-1}$. Now consider L_u and L_t for $u \neq t$. When L_u and L_t are superimposed, let the symbol x of L_u occur with the symbol y of L_t in the cell (i, j). Then

$$\alpha_x = \alpha_u \alpha_i + \alpha_j, \qquad \alpha_y = \alpha_t \alpha_i + \alpha_j$$

Hence

$$\alpha_i = \frac{\alpha_x - \alpha_y}{\alpha_u - \alpha_t} \qquad \alpha_j = \frac{\alpha_y \alpha_u - \alpha_x \alpha_t}{\alpha_u - \alpha_t}$$

Thus there is a uniquely determined cell (i, j) in which x of L_u occurs with y of L_t. Thus L_u and L_t are orthogonal.

Example

(i) Let $v = 4$. The elements of $GF(2^2)$ are $\alpha_0 = 0, \alpha_1 = 1, \alpha_2 = x, \alpha_3 = x+1$ where the addition and multiplication table is given in the previous lecture. We get the following 3 m.o.L.S. of order 4.

L_1				L_2				L_3			
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

(ii) For any given GF(v) we can choose a minimum function $f(y)$ such that $\alpha_0 = 0$, $\alpha_1 = y^0 = 1$, $\alpha_2 = y, \ldots, \alpha_{v-1} = y^{v-2}$ are all the elements of GF(v). Consider the Latin squares $L_1, L_2, \ldots, L_{v-1}$. They all contain the symbols, 0, 1, ..., v-1 in the natural order in the initial row. For $i \neq 0$ the ith row of L_1 contains the symbol x in column j where

$$\alpha_x = \alpha_i + \alpha_j$$
$$= y^{i-1} + y^{j-1}$$

Since $y^{i-1} + y^{j-1} = y.\ y^{i-2} + y^{j-1}$, the cell (i-1, j) of L_2 also contains the same symbol x. It is similarly obvious that the row i of L_{u+1}, u = 1, 2, ..., v-2 is the same as the row (i+1) of L_u if i=1,2 ..., v-2 and the row v-1 of L_{u+1} is the same as row 1 of L_u. Thus all the Latin squares can be obtained from L_1 which we may call the key square by cyclic permutation of the last (v-1) rows.

Further Reading

1. H.B.Mann : Design and analysis of experiments (Dover)
2. R.C.Bose : On the application of properties of Galois fields to the problem of construction of hyper-Graeco Latin squares, Sankhya 3(1938), 328-338.
3. R.C.Bose and K.R.Nair: On complete sets of Latin squares, Sankhya Sankhya 5 (1941) , 361-382.
4. O.Veblen and F.H.MacLagan-Wedderburn : Non-Desarguesian and non-Pascalian geometrics, Trans. Amer. Math. Soc. 8 (1907), 379-388.
5. S.S.Shrikhande : A note on mutually orthogonal Latin square (to appear in coming issue of Sankhya, (1961).

Finite planes and balance incomplete block designs

A. Finite projective planes

1. Finite projective planes. Consider a system containing a set of distinct elements called 'points' and certain distinct subsets of them called 'lines' together with an incidence relation (a point incident with a line i.e., passing through a point and a line incident with a point i.e., lying on a line or a line incident with a point i.e., passing 'through a point'). A number of points will be said to be collinear if they are incident with the same line. Similarly a number of lines will be said to be concurrent if they are incident with the same point. The system of lines and points will be said to form a projective plane $\sum$ if the following axioms are satisfied.

P_1 Any two distinct points are incident with one and only one line.

P_2 Any two distinct lines are incident with one and only one point.

P_3 There exist four points no three of which are collinear.

The unique line incident with two distinct points will be called the line containing these two points. Similarly the unique point incident with two distinct lines will be called the point of intersection of these lines.

Let X_1, X_2, X_3, X_4 be four points such that no three are collinear, where existence is guaranteed by P_3. Consider the six lines obtained by joining the different pairs.

l_1 : X_1 X_2 Z_1

l_2 : X_1 X_3 Z_2

l_3 : X_1 X_4 Z_3

l_4 : X_2 X_3 Z_3

l_5 : X_2 X_4 Z_2

l_6 : X_3 X_4 Z_1

These lines are distinct for otherwise three of the four points will be collinear. Let Z_1, Z_2 and Z_3 be the points of intersection as indicated. Then Z_1, Z_2, Z_3 are distinct from the X's and also from each other. For if Z_1 is identical with X_1 say, then from l_6 X_1, X_3, X_4 are collinear which is a contradiction. Similarly if Z_1 is the same as Z_2 then the lines l_1 and l_2 are both incident with the two distinct points X_1 and Z_1 which is again a contradiction.

Consider the lines l_1, l_2, l_5 and l_6. Obviously no three of them pass through a common point. Hence we have

Lemma 1: There exist four lines no three of which are concurrent.

Now consider any line of the system. If it is one of the six lines above, then it contains at least three points. If l is a line distinct from the above six lines, then it does not pass through at least one of the points say X_3 or X_4. If l does not pass through X_3, then it meets the three lines through X_3 in three distinct points. Similarly if it does not pass through X_4 it meets the three lines through X_4 given above in three distinct points. Hence we have

Lemma 2: Every line is incident with at least three points.

If we interchange the roles of points and lines and also interchange the phrases 'a point incident with a line' and 'a line incident with a point', then the statements P_1 and P_2 are interchanged so also are P_3 and lemma 1. This leads to the concept of duality as explained below. Let $\sum$ be a projective plane as defined above. Let (X_i) be the set of points of and (l_j) be the set of lines of $\sum$. Let $\sum'$ be another system of points and lines (L_j) and (x_i) respectively such that there is a one-to-one mapping $X_i \leftrightarrow x_i$, $l_j \leftrightarrow L_j$ between points and lines of $\sum$ with lines and points of $\sum'$ such that if X_i is incident with l_j in $\sum$, then the point L_j is incident with x_i in $\sum'$. Then we assert that $\sum'$ is also a projective plane which is called the dual of $\sum$. For suppose the points L_1 and L_2 of $\sum'$ are incident with two lines x_i and x_j of $\sum'$,

then by our correspondence, the points X_i and X_j of Σ' are incident with lines l_1 and l_2 of Σ, which is a contradiction. This varifies P_1 for Σ'. Similarly P_2 and P_3 are verified. It is obvious that the dual of Σ', denoted by $(\Sigma')'$ is identical with Σ.

Any theorem about Σ is a true statement about points and lines together with some incidence relation. The statement dual to this will be a statement obtained by interchanging points and lines and at the same time interchanging the phrases 'point incident with a line' and 'line incident with a point'. Obviously the dual statement will be true in Σ'. For example consider lemma 2, which is true in Σ and also in Σ' which also is a projective plane. Since Lemma 2 holds in Σ', its dual will be true in Σ, since $(\Sigma')' = \Sigma$. Hence in Σ we get

Lemma 3. Every point is incident with at least three lines.

This illustrates the important fact that if a theorem is true in Σ, then its dual is also true in Σ.

We will be interested mainly in finite projective planes which satisfy the following additional axiom.

P_4 There is at least one line incident with a finite number of points.

We state the following important theorem.

Theorem 1. Let $n \geq 2$ be an integer. In a projective plane Σ the following properties are equivalent.

1) There exists a line incident with exactly n+1 points.
2) Every line is incident with exactly n+1 points.
3) Every point is incident with exactly n+1 lines
4) There exists one point incident with exactly n+1 lines
5) There are in all $n^2 + n + 1$ points in Σ
6) There are in all $n^2 + n + 1$ lines in Σ

Proof. We first prove 1) --> 2) --> 3) --> 4) --> 1). Suppose l_1 is a line of Σ containing n+1 points where $n \geq 2$ by lemma 2.

By P_3 there exist two points X_3, X_4 not in l_1. Let the line $X_3 X_4$ meet l_1 in Z_1 and let X_1, X_2 be two points of l_1 other than Z_1. Let $X_1 X_3$ and $X_2 X_4$ meet in Z_2. Then obviously Z_2 is neither on l_1 nor on the line $X_3 X_4$. In particular the points X_3, X_4 and Z_2 are noncollinear. If A is any point not on l_1 then by joining A to each of the n+1 points of l_1, we get exactly n+1 lines incident with A. In particular there are exactly n+1 lines through each of the points X_3, X_4, Z_2. Similarly if there are exactly n+1 lines through a point, then any line not through that point contains exactly n+1 points. Since at least one of the points X_3, X_4 and Z_2 in not incident with any given line, it follows that every line contains exactly n+1 points. Thus 1) --> 2). Now take any point A whatsoever. From Lemma 1 there exists at least one line not incident with A. Hence joining A to the n+1 points of this line we get exactly n+1 lines incident with A. Thus 2) --> 3. Trivially 3) --> 4. Thus 1) --> 4) both in $\sum$ and $\sum'$. Taking the dual of 1) --> 4) in $\sum'$ we get 4) --> 1) in $\sum$. Thus 1), 2), 3), 4) are equivalent statements.

Now suppose 4) holds, then through each point there are exactly n+1 lines, accounting for all the points. Since each line contains exactly n points besides A, the total number of points is $n(n+1)+1 = n^2 + n + 1$. Thus 4) --> 5), in $\sum$. Since 1) --> 4) we have 1) --> 5) in $\sum'$, and hence by duality 4) --> 6) in $\sum$. Thus any one of the first four statements implies the last two statements. Now if 5) holds, then 1) holds for some $m \geq 2$. Hence the total number of points is $n^2 + n + 1 = m^2 + m + 1$ whence $m=n$. Hence the total number of lines is also $n^2 + n + 1$. Hence 5) implies all the rest. From duality therefore, 6) implies all the rest.

This completes the proof of the theorem.

A finite projective plane with n+1 points on a line is called a projective plane of order n.

2. Example of a projective plane of order 2. Consider four points X_1, X_2, X_3, X_4 such that no three are collinear. Then as in Section 1, we get 6 lines $l_1 \ldots, l_6$ and three additional points Z_1, Z_2, Z_3. Postulate a new line m. Containing the three points Z_1, Z_2, Z_3. Then is is easy to verify that these seven points and seven lines form a finite projective plane.

3. Finite projective planes based on Galois fields. Let $s = p^n$ where p is a prime and n is any positive integer. Then there exists a Galois field $GF(p^n)$. An ordered triplet $(x, y, z) \neq (o, o, o)$ with x, y, z in $GF(p^n)$ will be said to define a point. Two triplets (x_1, y_1, z_1) and (x_2, y_2, z_2) define the same point if and only if there exists a non-zero element α of the field such that $x_2 = \alpha x_1$, $y_2 = \alpha y_1$, $z_2 = \alpha z_1$. A linear homogeneous equation $ax + by + cz = 0$ where $(a, b, c) \neq (o, o, o)$ with a, b, c in the field defines a line. Further, $a_1x + b_1y + c_1z = 0$ and $a_2x + b_2y + c_2z = 0$ are said to define the same lines if and only if, there exists a non-zero element α of the field such that

$$a_2 = \alpha a_1, \quad b_2 = \alpha b_1, \quad c_2 = \alpha c_1$$

The point (x_o, y_o, z_o) will be said to be incident with the line $ax + by + cz = 0$ if and only if

$$ax_o + by_o + cz_o = 0$$

is true.

Consider two distinct points (x_1, y_1, z_1) and (x_2, y_2, z_2). Since the rank of the matrix

$$\begin{pmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{pmatrix}$$

is neither 0 nor 1, it is 2. Hence the homogeneous equations

$$ax_1 + by_1 + cz_1 = 0$$
$$ax_2 + by_2 + cz_2 = 0$$

have exactly one nontrivial solution for (a, b, c) all other solutions being non-zero multiples of this solution. Hence there is exactly one line of the system which contains these two points, thus verifying P_1. Similarly it is easy to verify P_2.

Consider the four points (1, 0, 0), (0, 1, 0), (0, 0, 1) and (1, 1, 1). The rank of the matrix

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

is obviously three. Hence there exists no line of the system which contains any three of these points. This verifies P_3.

Now consider the line $x = 0$ which is satisfied by (o, y, z) with $(y, z) \neq (o, o)$. Since (o, y, z) and $(o, \alpha y, \alpha z)$ represent the same point for $\alpha \neq 0$, it is easy to see that there are exactly $\frac{s^2-1}{s-1} = s+1$ points on this line. It now follows from Theorem 1, that the system defined is the projective plane of order s. Such a plane based on $GF(p^n)$ is called $PG(2,p^n)$.

Exercises

1) Construct $PG(2, 3)$ and $PG(2,2^2)$.

2) Verify that the lines $l_1,\ldots,l_7$ given below define a projective plane of order 2.

l_1	l_2	l_3	l_4	l_5	l_6	l_7
1	2	3	4	5	6	7
2	3	4	5	6	7	1
4	5	6	7	1	2	3

For finite projective planes $PG(2,p^n)$ it is easy to prove the following theorem which holds in ordinary plane geometry.

Desargues theorem. If $A_1\ A_2\ A_3$ and $B_1\ B_2\ B_3$ are two triangles

in perspective ..e., if the lines $A_i B_i$, i= 1,2,3 pass through a common point then the points of intersection (A_1A_2, B_1B_2), (A_1A_3, B_1B_3) and (A_2A_3, B_2B_3) are collinear.

It is known that if Desargues theorem holds for a finite projective plane, then it may be obtained with the help of finite field as we have done. However non-Desarguesian planes of order p^{2r} where p is an odd prime are known to exist. Also such planes of order 2^r, $r \geq 4$ exist. There is as yet no known example of finite projective plane whether Desarguesian or otherwise which is not of primepower order. A finite projective plane of non-prime-power order if it exists, must necessarily be non-Desarguesian.

2. Nonexistence of finite projective planes. We give here the proof by Chowla and Ryser of the only result on the nonexistence of finite projective planes due to Bruck and Ryser.

Theorem 2. If $n \equiv 1$ or 2 mod 4 and the square free part of n contains a prime congruent to 3 mod 4, then there does not exist a finite projective plane of order n.

Proof: Suppose a projective plane $\sum$ of order n exists. Put $N = n^2 + n + 1$ and number the points and lines of $\sum$ in any arbitrary manner. Define the incidence matrix A of the system $\sum$ by $A = (a_{ij})$ where

$a_{ij} = 1$ if the ith point is on jth line
$= 0$ otherwise.

Then if A' is the transpose of A, we have

$$A'A = AA' = C = (c_{ij})$$

where $c_{ij} = n+1$ if $i = j$
$= 1$ if $i \neq j$

Define the non-vector $\underline{L} = (L_1, \ldots, L_N)$ by

$$\underline{L} = \underline{x} A$$

where $\underline{x} = (x_1, \ldots, x_N)$ is a row of indeterminates.

Then

$$\begin{aligned}
\underline{L}\ \underline{L}' &= \underline{x}\, A\, A' \underline{x}' = \underline{x}\, C\, \underline{x}' \\
&= (n+1) \sum x_i^2 + 2 \sum_{i<j} x_i x_j \\
&= n \sum x_i^2 + \left(\sum x_i \right)^2 \\
&= n\left(x_2 + \frac{x_1}{n}\right)^2 + \ldots + n\left(x_N + \frac{x_1}{n}\right)^2 + (x_2 + \ldots + x_N)^2 \\
&= y_1^2 + n(y_2^2 + \ldots + y_n^2) \qquad \text{(I)}
\end{aligned}$$

where $y_1 = x_2 + \ldots + x_N$, and $y_i = x_i + x_1/n$, $i = 2,3,\ldots,N$. If $n=1$ or $2 \bmod 4$, then $N = 3 \bmod 4$. We now use the following results in number theory due to Lagrange.

Every positive integer can be written as a sum of four squares. Hence

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2$$

Product of two sums of four squares is a sum of four squares.

$$\begin{aligned}
&(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) \\
&= (a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4)^2 + (a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3)^2 \\
&+ (a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4)^2 + (a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2)^2 \\
&= c_1^2 + c_2^2 + c_3^2 + c_4^2 .
\end{aligned}$$

It is obvious that C's are rational functions of b's and a's.

Applying these two results to (I) we get

$$\sum L_i^2 = z_1^2 + z_2^2 + \ldots + z_{N-2}^2 + n(z_{N-1}^2 + z_N^2)$$

Since each L_i was a rational function of x's, it is also a rational function of the y's and finally of z's which are independent indeterminates. Since (I) is an identity it remains valid if some of the z's are specialised as linear combinations of the rest. Suppose in (I) that

$$L_1 = d_1 z_1 + \ldots + d_N z_N$$

Put $L_1 = z_1$ if $d_1 \neq 1$ and $L_1 = -z_1$ if $d_1 = 1$. This gives $L_1^2 = z_1^2$. Hence with this specialisation

$$L_2^2 + \ldots + L_N^2 = z_2^2 + \ldots + z_{N-2}^2 + n(z_{N-1}^2 + z_N^2)$$

continuing, we put $L_2 = \pm z_2, \ldots L_{N-2} = \pm z_{N-2}$ and we get

$$L_{N-1}^2 + L_N^2 = n(z_{N-1}^2 + z_N^2)$$

where L_{N-1} and L_N are rational linear forms in z_{N-1} and z_N. Since z_{N-1}, z_N are at our disposal, taking them as positive integers which are multiples of the denominators in L_{N-1} and L_N, the above relation becomes one in which all quantities are integers. Hence n is the quotient of two integers each of which is a sum of two squares i.e. $n=(x^2+y^2)/(u^2+v^2)$. We make use of the following result in the theory of numbers.

A positive number f is the sum of two squares if and only if the square free part of f contains no prime of the form $4m + 3$.

Hence the square free parts of $x^2 + y^2$ and $u^2 + v^2$ both contain only primes of the form 2 and $4m + 1$. Therefore square-free part of $n = (x^2 + y^2)/(u^2 + v^2)$ contains no prime of the form $4m + 3$. Hence n can be represented as the sum of two squares. If n_1 is the square-free part of n, then from the above result n_1 is also representable as the sum of two squares. But by our hypothesis n_1 contains a prime of the form $4m+3$ which implies that n_1 cannot be so represented. This completes the proof of the theorem.

B. Balanced Incomplete Block Designs

A balanced incomplete block design is an arrangement of v symbols (treatments) in b subsets (blocks) of k distinct symbols ($k < v$) satisfying the conditions that any two distinct treatments

occur together in exactly λ blocks. It then follows that each treatment occurs in exactly r blocks and that

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

Let A be the incidence matrix of the design with v rows and b columns, where $A = (a_{ij})$ and

$a_{ij} = 1$ if treatment i occurs in block j
$= 0$ otherwise.

Then if A' is the transpose of A

$$AA' = (r - \lambda)\, I_v + \lambda\, J_v$$

where J_v is a square matrix of order v with all elements one. Further

$$|\, AA' \,| = (r - \lambda)^{v-1} \, [\, r + \lambda(v-1)]$$
$$= (r - \lambda)^{v-1} \, rk \neq 0$$

since $r = \lambda$ implies $v = k$. Hence rank $(A) \leq \min(v, b)$. This implies the well known inequality $v \leq b$ due to Fisher.

A b.i.b.d. is called resolvable if the blocks can be separated into sets such that each set is a complete replication, i.e. contains all the treatments exactly once. Necessarily k must be a factor of v and it can be easily shown that Fisher's inequality can be strengthened to $b \geq v + r - 1$.

A b.i.b.d. is called symmetric if $b = v$ and hence $r = k$. Then

$$|A\, A'| = |\, A \,|^2 = (r - \lambda)^{v-1} \, r^2.$$

Hence $(r - \lambda)^{v-1}$ must be a perfect square. Thus if v is even we get the following important result.

Theorem 3. A necessary condition for the existence of a symmetric b.i.b.d. when v is even is that $r - \lambda$ must be a perfect square.

For a symmetric design $r = k$ and hence

$$J_v A = kJ_v = rJ_v = \lambda J_v$$

Hence

$$AA'A = (r - \lambda)A + \lambda AJ_v$$

and since A is a square non-singular matrix we get

$$A'A = (r - \lambda)I_v + \lambda J_v$$

which implies that any two blocks of the design have exactly λ treatments in common. Hence we have

Theorem 4. In a symmetric b.i.b.d. if any two treatments occur together λ times, then any two blocks have exactly λ treatments in common.

Let D be any design with parameters v, b, r and k. We can form the dual configuration with parameters $v' = a$, $b' = v$, $r' = k$, $k' = r$ in the following manner. Let the treatments and blocks of D correspond in one-to-one manner to the blocks and treatments of D' such that if a treatment of D lies in a block of D, then in D' the corresponding block contains the corresponding treatment. Thus if D is configuration given by the following arrangement of 4 treatments in 6 blocks

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

then D' is the arrangement given by

1	1	2	3
2	4	4	5
3	5	6	6

In general if D is a b.i.b.d., then D' is not necessarily a b.i.b.d. It is obvious that if A is the incident matrix of D, then A' is the incidence matrix of D'. In particular if v=b, we get from the previous theorem, the following result.

Theorem 5. The dual of a symmetric b.i.b.d. is also a symmetric b.i.b.d. with the same parameters.

From a symmetric design (v, k, λ) by omitting a block and all treatments contained therein and making use of Theorem 4, we get another b.i.b.d. with parameters.

$v' = v-k$, $b' = v-1$, $r=k$, $k' = k-\lambda$, $\lambda' = \lambda$ which may be called the derived design of the original (v, k, λ) design. Similarly by omitting a block and retaining only the treatments of this block in the retained blocks we get another b.i.b.d. with parameters.

$v'' = k$, $b'' = v-1$, $r'' = k-1$, $k'' = \lambda$, $\lambda'' = \lambda - 1$

which may be called the residual design of the original symmetric design.

Thus from a symmetric b.i.b.d. we can always construct its derived design. In general it is not possible to reverse this process. It has however been shown that for the case $\lambda = 1, 2$, it is possible to construct in a unique manner the symmetric design given a design corresponding to the parameters of its derived design and hence we have

Theorem 6. For $\lambda = 1, 2$, b.i.b.d. (v, k, λ) and its derived design are either both existent or both nonexistent.

Corollary. Designs $v = b = s^2 + s + 1$, $r = k = s + 1$, $\lambda = 1$ and $v = s^2$, $b = s^2 + s$, $r = s + 1$, $k = s$, $\lambda = 1$ are either both existent or both nonexistent.

Analogous to Theorem 2, we have the following result on the impossibility of (v, k, λ) design.

Theorem 7. Let p be any prime factor of the square-free part of $k - \lambda$. Then a necessary condition for existence of (v, k, λ) design is that

$$(\lambda/p) = 1 \text{ if } v = 1 \text{ mod. } 4$$

and $$(-\lambda/p) = 1 \text{ if } v = 3 \text{ mod. } 4$$

where (a/p) denotes the quadratic character of a with respect to p.

We omit the proof of this theorem, given by Chowla and Ryser (1950), Shrikhande (1950).

Systematic methods of construction of b.i.b. designs were given by Bose (1939).

C. Connection between finite projective planes and complete sets of m.o. L.S.

We have seen that if $s = p^n$, we can construct a complete set of m.o.L.S. of order s as also a finite projective plane PG(2, s). The relation between a complete set of m.o.L.S. of order s and a finite projective plane of order s is however more fundamental than the constructions based on GF(s). Specifically we have

Theorem 8. Existence of a finite projective plane of any order v is equivalent to the existence of a complete set of m.o.L.S. of order v.

Proof. Let l be any line of the projective plane and X_R, X_C, X_1, ..., X_{v-1} be the points on l. The $v^2 + v$ lines other than l can be separated into (v+1) groups of v each, such that any two lines of the same set intersect in some point X, on l whereas two lines from different sets intersect in a point not on l. If we omit the line l and the points lying on it and call the remaining points and lines as finite points and finite lines, then the finite lines can be separated into pencils of parallel lines $[X_R]$, $[X_C]$, $[X_1]$,... $[X_{v-1}]$. Number the lines of each pencil in any arbitrary manner by the integers 1, 2, ..., v. We can use the points of intersections of the pencils $[X_R]$ and $[X_C]$ to coordinatise the cells of a v x v square. Corresponding to the pencil $[X_\alpha]$ $\alpha = 1, 2, \ldots, v-1$, we form a square by putting in the cell (i, j), the number corresponding to that line of $[X_\alpha]$ which passes through the point corresponding to the cell (i,j). It is easy to verify that square L_α is a Latin Square. Since through each finite point there passes a unique line of the different pencils, and two lines of different pencils uniquely determine a finite point, it is easy to verify that the latin squares thus obtained are mutually orthogonal.

Conversely suppose we are given a set $L_1, L_2, \ldots, L_{v-1}$ of v-1

m.o.L.S. of order $v, (v \geq 2)$ in integers 1, 2, ..., v. Write down two squares $L_R(L_C)$, of order v containing the symbol i in row (column) numbered i and write down a square L of order v containing distinct symbols x_i, $i = 1, 2, \ldots, v^2$. For each j; $j = R, C, 1, 2, \ldots, v-1$, form v blocks corresponding to the same symbol of L_j when L_j is superposed on L. It is easy to verify that we get a b.i.b design with parameters

$$v' = v^2,\ b' = v^2 + v,\ r' = v+1,\ k' = v,\ \lambda = 1,$$

in which the blocks corresponding to each j form a complete replication. Adding the symbol θ_j to all the blocks corresponding to L_j and adding a new block containing $(\theta_R, \theta_C, \theta_1, \ldots, \theta_{v-1})$ one easily verifies that we get a b.i.b.d. with parameters

$$v' = b' = v^2 + v+1,\ r' = k' = v+1,\ \lambda = 1$$

which is easily verified to be a finite projective plane of order v.

This result combined with Theorem 3 of the previous lecture and Theorem 2 of the present lecture gives the following

Corollary: If $n = 1$ or $2 \bmod 4$ and the square-free part of n contains a prime $= 3 \bmod 4$, then $N(n) \leq n-4$.

D. Finite Euclidean Planes

1. Consider a class of elements called points and a class of subsets of these called lines and an incidence relation such that a point and a line may or may not be incident. Two lines will be called parallel if there is no point incident with both of them. The sets of points and lines form a finite Euclidean plane if the following axioms are satisfied.

E_1 There is exactly one line incident with any two distinct points.

E_2 Given a point P not incident with a line l, there exists just one line incident with P and parallel to l.

E_3 There exist at least three points not incident with the same line.

E_4 There exists at least one line incident with finite number of points.

Let l, m, n be distinct lines such that l, and m are parallel and also l and n are parallel. Then if m and n are not parallel, there is a point P not on l, such that m and n pass through P, but this contradicts E_2. Hence we have

Lemma 1. If two lines are each parallel to a third line, they are parallel with each other.

This theorem can be used to divide all the lines of the plane into sets called parallel pencils, such that any two distinct lines of a parallel pencil are parallel; whereas any two lines belonging to different pencils are non-parallel, i.e., they have at least one point in common. It is easy to prove the following.

Lemma 2. There is exactly one line in any parallel pencil which passes through a given point P.

To study the properties of an Euclidean plane, it is convenient to first embed it in a corresponding projective plane which can be done in the following manner. Corresponding to each pencil of parallel line we postulate the existence of a point called the vertex of the pencil, such that the vertex is incident with every line of the pencil. We may call these vertices as points at infinity and postulate the existence of a new line called the line at infinity which is incident with all the points at infinity and with no other points. We may call the original points and lines of the Euclidean plane as finite points and finite lines. It is easy to prove that this extended system of points and lines is a finite projective plane as follows.

Any two finite points or any two infinite points obviously determine a unique line. Suppose X is a point at infinity, then X is the vertex of a pencil and through any finite point P, there is one line of the

pencil corresponding to X. This is obviously the only line through P and X. Hence axiom P_1 is satisfied.

Any two finite parallel lines are incident with only the vertex of the corresponding pencil and any two finite non-parallel lines intersect in at least one point and hence exactly one point by E_1. Further any finite line l and the line at infinity have the vertex of the pencil corresponding to l as the only point of intersection. This verifies P_2.

By E_3 there exist three finite points X_0, X_1 and X_2 which are not collinear. Let V_1 be the vertex of the line X_0X_1 and V_2 the vertex of the line X_0X_2. Then obviously V_1, V_2 and X_1 are not collinear. Similarly V_1, V_2 and X_2 are not collinear. Further if X_1, X_2 and V_1 are collinear, then X_2 must lie on the line $X_0X_1V_1$ implying that X_0, X_1, X_2 are collinear, which is a contradiction. Similarly X_1, X_2 and V_2 are not collinear. Thus the points X_1, X_2, V_1 and V_2 satisfy axiom P_3. Since the number of points on any line of the extended system is finite, P_4 is also satisfied. This verifies that the extended system is a finite projective plane.

Conversely given a finite projective plane, we can obtain the finite Euclidean plane by omitting a line and all the points lying on it.

By embedding the finite Euclidean plane into the corresponding projective plane, it is easy to prove the following.

Theorem 9. In a finite Euclidean plane.

i) There is exactly one point incident with two non-parallel lines.

ii) Each line is incident with exactly s points and each point is incident with exactly s+1 lines where s is an integer greater than or equal to 2.

iii) The total number of points is s^2, and the total number of lines is s^2+s, which can be divided into s+1 parallel pencils, each containing a set of s mutually parallel lines.

It is obvious that regarding points and lines as treatments and blocks, a finite Euclidean plane gives rise to a b.i.b.d. with

$$v = s^2,\ b = s^2 + s,\ r = s+1,\ k = s,\ \lambda = 1.$$

Conversely given a b.i.b.d. with above parameters and regarding treatments and blocks as points and lines respectively we have a system of points and lines for which E_1 is obviously true. Now consider any line say 1, containing the points $X_1, X_2, \ldots, X_s$ say and let P be a point not on 1, then since $\lambda = 1$, there exist s distinct lines through P each containing exactly one point X_i, $i = 1, 2, \ldots, s$. Hence the remaining line through P does not contain any point of 1 and hence is parallel to 1. This verifies E_2. The point P together with any two points of 1 obviously form a set of three non-collinear points verifying E_3. E_4 is obviously true. Thus the b.i.b.d. above is nothing but a finite Euclidean plane of order s(i.e., containing s points on each line).

2. Construction of a finite Euclidean plane based on Galois fields. Let $s = p^n$ and GF(s) be the Galois field with s elements. Define a point as any ordered pair (x, y) of elements of the field. Define a line as any ordered triplet (a, b, c) with $(a, b) \neq (0, 0)$. Two such triplets will be said to determine the same line if the ratio of corresponding components is the same non-zero element of the field. A point (x, y) is said to be incident with the line (a, b, c) if and only if

$$ax + by + c = 0$$

in the field.

Two lines (a_1, b_1, c_1) and (a_2, b_2, c_2) are said to be parallel if there exists $\alpha \neq 0$ in the field such that

$$a_1 = \alpha a_2,\ b_1 = \alpha b_2,\ c_1 \neq \alpha c_2$$

We verify that the points and lines so defined form a Euclidean plane.

Denote the line (a, b, c) by the more familiar notation $ax + by + c = 0$. Let (x_1, y_1) and (x_2, y_2) be two distinct points. Then if $x_1 = x_2$ and hence $y_1 \neq y_2$, the only line containing both points is the line $x - x_1 = 0$. Similarly if $y_1 = y_2$, the only line through both is $y - y_1 = 0$. If $x_1 \neq x_2$ and $y_1 \neq y_2$ then the line containing both the points is

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1)$$

This verifies E_1.

Let $P = (x_o, y_o)$ be a point not on the line l given by $ax + by + c = 0$, then it is easy to verify that the line m given by $ax + by - (ax_o + by_o) = 0$ is the only line through P which is parallel to l. This verifies E_2.

The points (1, 0), (0, 1), (0, 0) are obviously three points which are not incident with the same line, thus verifying E_3.

Finally the number of points on the line $x = 0$ is exactly s since all points on this line are given by (0, y) for any arbitrary y in GF(s): This verifies E_4.

The properties of the Euclidean plane mentioned in Theorem 9 can be directly verified. This is left as an exercise.

We denote the finite Euclidean geometry constructed with the help of the Galois field GF(s) by EG(2, s).

The correspondence between finite Euclidean and projective geometries EG(2, s) and PG(2, s) based on GF(s) can be carried out analytically as shown below :

	EG(2, s)	PG(2, s)
1.	Point: (x, y)	Point (x, y, 1) = (ex, ey, e), $e \neq 0$
		Point (x, y, 0) = (ex, ey, 0), $e \neq 0$
2.	Line: $ax + by + c = 0$ $(a, b) \neq (0, 0)$	Line $ax + by + cz = 0$
	-	Line $z = 0$
3.	Incidence : Point (x_0, y_0) lies on $ax + by + c = 0$	Point $(x_0, y_0, 1)$ lies on $ax + by + cz = 0$.

It is easy to verify that the correspondence gives the embedding of EG(2, s) in PG(2, s).

Exercise. Write down the points and lines of EG (2, 3) and EG(2, 4).

Further reading

1. R.D. Carmichael : Introduction to the theory of groups of finite order (Ginn and Co.), 1937.

2. Marshall Hall : The theory of groups, Macmillan (1959).

3. R.C.Bose : On the construction of balanced incomplete block designs. Ann. of Engen. I (1939), 353-399.

4. S. Chowla and H.J.Ryser : Combinatorial problems, Can. J. Math. 2 (1950), 93-99.

5. R.H.Bruck and H.J.Ryser: The nonexistence of certain finite projective planes, Can. J. Math. 1 (1949), 88- 93.

6. S. S. Shrikhande : The impossibility of certain symmetrical balanced incomplete block designs, Ann. Math. Stat. 21 (1950), 106-111.

Lecture 4

Some generalisation of Balanced Incomplete Block Designs

Group divisible design. An arrangement of v treatments in b sets each containing k distinct treatments is said to be a group divisible (GD) design if the treatments can be divided into e groups of m treatments each such that any two treatments belonging to the same group occur together in λ_1 blocks, and any two treatments from different groups occur together in λ_2 blocks. We will denote such a design by the notation GD(v; k, m; λ_1, λ_2). It is then obvious that

$$v = em,\ bk = vr,\ \lambda_1(m-1) + \lambda_2\, m(e-1) = r(k-1)$$

where r is the number of replications i.e., the number of times each treatment occurs in the design.

Number the treatments of the ith group by $(i-1)m+1 \ldots, im$, where $i = 1, 2, \ldots, e$ and define the incidence matrix of the design $A = (a_{ij})$ in the usual manner i.e.,

$a_{ij} = 1$ if ith treatment occurs in jth block

$= 0$ otherwise.

Then $A A' - \theta I_v = \begin{pmatrix} B & C & \cdots & C \\ C & B & \cdots & C \\ \vdots & \vdots & & \vdots \\ C & C & \cdots & B \end{pmatrix}$

where $B_{m\times m}$ has $r - \theta$ along the main diagonal and λ_1 elsewhere and $C_{m\times m}$ has all the elements λ_2.

Then

$$|A A' - \theta I_v| = |B - C|^{e-1} \, |B + (a-1)C|$$

$$= (P - \theta)^{e-1} \, (Q - \theta)^{e(m-1)} \, (rk - \theta)$$

where $P = rk - \lambda_2 v$ and $Q = r - \lambda_1$.

Hence since the characteristic roots of the matrix AA' are non-negative, we have

$$P \geq 0, \quad Q \geq 0.$$

The G.D. design can be divided into three classes

i) Regular (R) : characterised by $P > 0, Q > 0$

ii) Semiregular (SR): $P = 0, Q > 0$

iii) Singular (S) : $Q = 0$

We will be interested only in designs where $\lambda_1 = 0, \lambda_2 = 1$ which can be denoted by GD $(v; k, m; 0, 1)$.

We will not discuss here the questions of non-existence, construction and properties of such designs. A few references dealing with these questions are given at the end. We will however mention only a few properties that will be immediately useful to us.

We call a GD resolvable if it is possible to separate the blocks into sets such that each set is a complete replication.

Orthogonal array of strength 2: An arrangement of v distinct symbols in an array with k rows and v^2 columns is called an orthogonal array of strength 2 and index unity, if in any two rows of the array all possible v^2 ordered pairs (i, j) of the v symbols occur exactly once. We will denote such an array by the notation $[v^2, k, v, 2]$.

Theorem 1. Existence of k-2 m.o.L.S. of order v is equivalent to the existence of $[v^2, k, v, 2]$.

Proof. Let $L_1, \ldots, L_{k-2}$ be a set of m.o.L.S. of order v in integers 1, 2, ..., v. Let $L_R(L_C)$ be a square array containing i in the ith row (column) i = 1, 2, ..., v. Write each square as a row with v^2 entries such that the symbol in cell (i, j) occurs in the position numbered $(i - 1)\, v + j$. We then get a matrix with k rows and v^2 columns in integers 1, 2, ..., v. We assert that this forms $[v^2, k, v, 2]$. It is obvious that in rows corresponding to L_R and L_C, every ordered pair occurs exactly once. From the properties of a

Latin Square the same is true for row corresponding to $L_R (L_C)$ and any other row. For rows corresponding to L_i and L_j, $i \neq j = 1, 2, \ldots, k-2$ the result follows from the orthogonality of L_i and L_j. Hence the matrix is an orthogonal array $[v^2, k, v, 2]$. Conversely given $[v^2, k, v, 2]$, we can use any two rows (which can be taken as the first two rows) without loss of generality to coordinatise the cells of a square array of order v. Corresponding to any one of the remaining k-2 rows, we form a square by putting in the cell (i, j) the symbols which occurs in that rows in the corresponding position. We thus get k-2 squares $L_1, L_2 \ldots, L_{k-2}$ corresponding to rows numbered 3, 4,..., k. Since all the ordered pairs of v symbols occur exactly once in any two rows, considering the 1st row with any other row from the last k-2 rows, it is obvious that in each L_α, every symbol occurs exactly once in every row. Similarly considering the 2nd row with any of the last k-2 rows, each symbol occurs exactly once in every column of L_α. Thus each L_α is a Latin Square. Similarly by considering any two distinct rows out of the last k-2 rows, it is obvious that any two of the Latin Squares are orthogonal. Thus we get a set of k-2 m.o.L.S. of order v.

Theorem 2. Existence of an orthogonal array $[m^2, e, m, 2]$ implies the existence of a semiregular design GD(em; e, m; 0, 1) with parameters

$$v = em, \quad b = m^2, \quad r = m, \quad k = e, \quad \lambda_1 = 0, \quad \lambda_2 = 1$$

and conversely.

Proof. Identify the symbol θ in row i with the treatment numbered $(i-1)\, m + \theta$; $i = 1, 2, \ldots, e$; $\theta = 1, 2, \ldots, m$ and take the columns of the array as blocks of a design. The parameters v, b, r, k are easily verified. The m symbols in any row form a group of m treatments. It is obvious that two treatments belonging to the same group do not occur together in any block giving $\lambda_1 = 0$. Since any two rows contain all the ordered pairs exactly once, it is obvious that

two treatments coming from different groups occur together in exactly one block giving $\lambda_2 = 1$. Hence the design is a GD design with indicated parameters and is obviously a semi-regular design.

Conversely given the semi-regular GD with the indicated parameters, it follows from a result of Connor that each block contains exactly one treatment from each group. We number the treatments of the design so that the ith group contains treatments numbered $(i-1)m+\theta$ $\theta = 1, 2, \ldots, m$; $i = 1, 2, \ldots, e$. If a block (written as column) contains the treatment $(i-1)m + \theta$, replace it by the number θ which is put in row numbered i. It is now easy to verify that we get an orthogonal array $[m^2, e, m, 2]$.

Since an orthogonal array remains an orthogonal array if we discard a number of rows, from the above we have the

Corollary. Existence of an orthogonal array $[m^2, e, m, 2]$ implies the existence of a semi-regular GD$(qm; q, m; 0, 1)$ with parameters.

$$v = q\,m,\ b = m^2,\ r = m,\ k = q,\ \lambda_1 = 0,\ \lambda_2 = 1$$

for any $q \leq e$.

Theorem 3. The existence of e-2 m.o.L.S. of order m or equivalently the existence of $[m^2, e, m, 2]$ implies the existence of a resolvable semi-regular GD$((e-1)m, e-1, m, 0, 1)$ and conversely.

Proof. Consider any row, say the last row of $[m^2, e, m, 2]$. Then we can divide the m^2 columns into m sets of m columns each, such that the ith set contains the symbol i in the last row; i=1,2, ..., m. Omitting the last row, we have a resolvable array $[m^2, e-1, m, 2]$ in which the columns can be divided into m sets of m each such that in each set every row contains all the symbols 1, 2, ..., m exactly once. Applying the method used in Theorem 2 we get the required resolvable GD design.

Conversely given the resolvable GD, we can construct the resolvable array $[m^2, e-1, m, 2]$ as in Theorem 2. We can now add one more

row to the array by putting the symbol i in the new row in position corresponding to the ith set. We obviously get $[m^2, e, m, 2]$.

Pairwise balanced design of index unity. An arrangement of v objects (treatments) in b sets (blocks) will be called a pairwise balanced design of index unity and type $(v; k_1, k_2, \ldots, k_m)$ if each block contains either $k_1, k_2, \ldots, k_m$ distinct treatments ($k_i \leq v$, $k_i \neq k_j$) and every pair of distinct treatments occurs in exactly one block of the design. If the number of blocks containing k_i treatments is b_i, then obviously

$$b = \sum_1^m b_i, \quad v(v-1) = \sum_1^m b_i k_i (k_i - 1).$$

Consider a pairwise balanced design (D) of index unity and type $(v; k_1, k_2, \ldots, k_m)$. The sub-design (D_i) formed by blocks of size k_i will be called the ith equiblock component of (D), i =1, 2,..., m.

A subset of blocks of (D_i) will be said to be of type I if every treatment occurs in the subset exactly k_i times. Obviously the number of blocks in such a subset is v. As pointed out by Levi we can arrange the treatments within the blocks of the subset in such a way that every treatment occurs exactly once in every position. If the v blocks of the subset are written as columns, each treatment occurs exactly once in every row. When so written the blocks will be said to be in the standard form.

A subset of blocks of (D_i) will be said to be of type II if every treatment occurs exactly once in the subset. The number of blocks in the subset is obviously v/k_i.

The component (D_i) will be defined to be separable if the blocks can be divided into subsets of type I or type II (both types may occur in (D_i) at the same time). If r_i be the number of subsets of type I and s_i the number of subsets of type II, then clearly

$$v(r_i k_i + s_i) = k_i b_i$$

The design (D) is said to be separable if each (D_i) is separable. It then follows that

$$v-1 = \sum_{1}^{m} (r_i k_i + s_i)(k_i - 1)$$

The set of equiblock components $(D_1), (D_2), (D_e)$, is said to form a clear set, if no two blocks contain a common treatment. Clearly a necessary condition is

$$\sum_{1}^{e} b_i k_i \leq v.$$

We give below a number of examples of pairwise balanced designs which we will use later on.

Example 1. All b.i.b.d. are obviously pairwise balanced designs. Any symmetric b.i.b.d. has a set of blocks of type I and hence is separable. Similarly any resolvable b.i.b.d. has sets of blocks of type II only and is again separable. Further from a resolvable (v; k) with r replications we can get pairwise balanced designs of the type (v+1; k, k+1) and (v+x; k, k+1, x) for $1 < x < r$ and (v+r; k+1, r) in which the single block of size x or r forms a clear set. All we need do is to add a new treatment say θ to all the blocks of one replication or add new treatments $\theta_1, \theta_2, \ldots, \theta_x$; $1 < x \leq r$ one each to all the blocks of x chosen replications and further add a new block containing $\theta_1, \theta_2, \ldots, \theta_x$. Thus from the resolvable b.i.b.d. with parameters v = 15, b = 35, r = 7, k = 3, $\lambda_1 = 1$ we get (16; 3, 4) as also (22; 4, 7).

It is known that the resolvable design (6t + 3; 3) always exists where the number of replicationsis necessarily 3t + 1. All such designs can be used in a similar manner to give rise to other pairwise

balanced designs. If s is a prime power then we know that resolvable (s^2, s) exists. These designs can also be used in a similar manner.

Example 2. Consider designs (v, k). Let $\alpha_1, \alpha_2, \alpha_3$ be three treatments which do not occur in the same block. Then these are three distinct blocks containing exactly any two of these three treatments. By omitting these 3 treatments we get a pairwise - balanced design $(v-3; k, k-1, k-2)$ in which the blocks of size $k-2$ form a clear set. Thus from the design $(25; 5)$ we get the design $(22; 5, 4, 3)$ in which the blocks of size 3 form a clear set.

Example 3. From the GD$(v; k, m; o, 1)$ where $v = em$ by adding e additional blocks of size m corresponding to the groups we get a pairwise balanced design $(v; k, m)$ in which the e blocks of size m obviously form a clear set. If further the original GD design is separable, so is the design $(v; k, m)$ obtained from it.

Further reading

See references at the end of next lecture.

Lecture 5

Further results on mutually orthogonal Latin Squares.

We will indicate in this lecture further results on mutually orthogonal Latin Squares and in particular give disproofs of the conjectures of Euler and MacNeish.

Lemma 1. If orthogonal arrays $[v_1^2, k_1v_1, 2]$ and $[v_2^2, k_2, v_2, 2]$ exist and if $k = \min(k_1, k_2)$ then orthogonal array $[v_1^2v_2^2, k, v_1v_2, 2]$ exists.

Proof. Let the symbols of the two orthogonal arrays be denoted by $\alpha_1, \ldots, \alpha_{v_1}$, and $\beta_1, \ldots, \beta_{v_2}$. Retain only the first k rows of both the arrays. Let each column of the first array containing the symbols, say, $\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_k}$ be combined with each column of the second array containing the symbols, say, $\beta_{j_1}, \beta_{j_2}, \ldots, \beta_{j_k}$ to form a column containing the symbols $\alpha_{i_1}\beta_{j_1}, \alpha_{i_2}\beta_{j_2}, \ldots, \alpha_{i_k}\beta_{j_k}$. We thus get a matrix with $v_1^2 v_2^2$ columns and k rows containing the symbols $\alpha_i\beta_j$, $i = 1, \ldots, v_1$; $j = 1, \ldots, v_2$. It is easy to see that this matrix is an orthogonal array in the v_1v_2 symbols $\alpha_i\beta_j$.

Let any positive integer v be decomposed into its primepower decomposition $v = p_1^{n_1} p_2^{n_2} \ldots, p_u^{n_u}$. For each $p_i^{n_i}$ there exist $p_i^{n_i}-1$ m.o.L.S. Hence if we define

$$n(v) = \min (p_1^{n_1}, p_2^{n_2}, \ldots, p_u^{n_u}) - 1$$

using the equivalence of $[v^2, k, u, 2]$ with $k-2$ m.o.L.S. of order v, we have

Corollary 1. For any integer v, $N(v) \geq n(v)$.

Corollary 2. For any integer not of the form $4t + 2$, $N(v) \geq 2$

Corollary 3. $N(v_1v_2) \geq \min (N(v_1), N(v_2))$.

Corollary 1 was first proved by MacNeish in 1922, who conjectured that $N(v) = n(v)$ for all v. This is known as MacNeish's conjecture. Since $n(4t + 2) = 1$, MacNeish's conjecture implies that there do not exist 2 m.o.L.S. of any order $4t+2$, which is known as Euler's conjecture made in 1782. At Czar's court Euler was asked to arrange 36 officers belonging to 6 different ranks and 6 different regiments in a square array of order 6 so that each rank and each regiment is represented exactly once in every row and every column. This problem is equivalent to constructing two m.o.L.S. of order 6. Euler did not succeed in giving a solution to this problem and made the conjecture that the problem is incapable of solution for the number 6, as also for all the numbers of the form $4t+2$, $t \geq 2$. Several attempts have been made in the past to prove Euler's conjecture (Peterson, Wernicke, MacNeish). They were however all erroneous, as we will show that Euler's conjecture is totally false for all numbers > 6. For $v = 2$, Euler's result is trivial, and for the number 6 it was verified by Tarry and later on by Fisher and Yates by the process of complete enumeration. MacNeish's conjecture was first disproved by Parker (1958). Bose and Shrinkhande generalised his methods to provide further counter examples and also to disprove Euler's conjecture. Subsequently the three authors completely disproved Euler's conjecture for all numbers excepting 2 and 6. Utilising the results of these three authors, Chowla, Erdos and Straus (1960) have proved that $N(v) \to \infty$ as $v \to \infty$, which in essence implies that $N(v)$ cannot be expressed in terms of the minimum factor in the primepower decomposition of v.

Let G be a permutation group on letters $x_1, x_2, \ldots, x_n$. Then G is said to be a doubly transitive group on the n letters if (i) for any x_i and x_j there exists a σ in G, such that $(x_i)\sigma = x_j$ and (ii) any ordered pair (x_i, x_j) $i \neq j$ is taken into any other ordered pair (x_α, x_β) $\alpha \neq \beta$ by some element of G. We will consider such doubly transitive groups in which only the identity permutation fixes

two letters. It is then obvious that there is exactly one permutation in G which carries a given ordered pair into any other given ordered pair. It is known that such a doubly transitive group exists if and only if n is a primepower p^r. Since a finite field GF(n) exists, an analytical construction of such a group is provided by the group of linear transformations $Y_i = \alpha x_i + \beta$, $i = 1, 2, \ldots, n$ and $\alpha \neq 0, \beta, x_i, y_i$ in GF(n). Let P be the matrix of order n x n(n-1) when the permutations are written as columns. Then obviously $P = (P_1, P_2, \ldots, P_{n-1})$ where each P_i contains all the symbols exactly once in every row and in any two rows of P every ordered pair (x_i, x_j), $i \neq j$ occurs exactly once. Let P_o be the square matrix of order n with element x_i in the ith column. Then obviously $A = [P_o, P]$ is an orthogonal array $[n^2, n, n, 2]$, in which the n^2 columns can be divided into n sets of n each such that each of the n symbols occurs exactly once in every row of each set. It is now obvious that we can add one more row in a trivial manner to get $[n^2, n+1, n, 2]$ which implies the existence of n-1 m.o.L.S. of order n.

If in the above we do not insist on the columns of P forming a group of permutations, we have the concept of a doubly transitive set in which the columns are permutations of n symbols such that each ordered unlike pair (x_i, x_j), $i \neq j$ is carried into every other ordered unlike pair exactly once. Such a doubly transitive set also gives rise to a set of n-1 m.o.L.S. of order n. Conversely given a complete set of m.o.L.S. of order n which can be taken in the standard form, we can take a square of order n containing x_i in the ith column and form the array $[n^2, n, n, 2]$ in which there exist n columns each containing the same symbol x_i in every position. By omitting these columns we are left with a doubly transitive set P. Thus the problem of constructing a complete set of m.o.L.S. of order n is exactly equivalent to constructing the corresponding doubly transitive set P in n symbols. As yet there is no case known where such a P can be constructed for n different from a primepower.

We prove the following improved version of a result due to Parker.

Theorem 1. Suppose a design $(v; k)$ exists where k is a prime-power, then $N(v) \geq k-2$. If the design is separable, then $N(v) \geq k-1$.

Proof. Suppose $(v; k)$ exists where k is a primepower. Consider the matrix P of order k by $k(k-1)$ constructed in k symbols, $1, 2, \ldots, k$. Let δ be any block of the design written as a column which contains the treatments $t_{i_1}, t_{i_2}, \ldots, t_{i_k}$ in positions $1,2,\ldots,k$ respectively. Denote by $P(\delta)$ the matrix obtained from P by replacing the integer j by the symbol t_{i_j} which occurs in δ in the jth position. Then since the ordered pair (α, β), $\alpha \neq \beta = 1, 2, \ldots, k$ occurs exactly once as a column in any two rows of P, the ordered pair $(t_{i_\alpha}, t_{i_\beta})$ also occurs exactly once in any two rows of $P(S)$. Hence denoting by D the design (v, k) and by $\Delta = P(D)$ the corresponding matrix with k rows and $bk(k-1) = vr(k-1) = v(v-1)$ columns, where b is the number of blocks in D, it is easy to see that in any two rows of Δ every ordered pair (t_α, t_β), $\alpha \neq \beta = 1, 2, \ldots, v$ occurs exactly once. Let Δ_o be the $k \times k$ matrix containing t_α in αth column, $\alpha = 1, 2, \ldots, v$. Then obviously

$$(\Delta_o, \Delta)$$

is an orthogonal array $[v^2, k, v, 2]$ which implies the existence of $k-2$, m.o.L.S. of order v. Thus $N(v) \geq k-2$.

To consider the second part, suppose $D = (D_{\alpha_1}, \ldots, D_{\beta_1} \ldots)$ where each D_α is a set of blocks of type I, which can be taken in the standard form, and each D_β is a set of blocks of type II. Since each row of D_α contains all the v symbols exactly once, it is obvious that the v columns obtained by operating any column of P on D_α, contain all the v symbols exactly once. Now consider any D_β which contains v/k columns such that in these columns all the v symbols occur exactly once. Let $P = (P_1, P_2, \ldots, P_{k-1})$, where each P_i contains all the k symbols exactly once in every row. Then it is obvious that

$P_i(D_\beta)$ contains v columns such that in each row each of the v symbols occurs exactly once. It then follows that $\Delta - P(D)$ can be broken up into (v-1) sets of v columns each such that every row of each set contains all the symbols exactly once. It then follows that (Δ_o, Δ) is a resolvable orthogonal array with k constraints to which one more row can be added in an obvious manner giving $N(v) \geq k-1$.

Since symmetric b.i.b.d. and resolvable b.i.b.d. are obviously separable we have,

Corollary 1. Existence of a symmetric or resolvable (v; k) and k a primepower implies

$$N(v) \geq k-1.$$

Example 1. From symmetric (21; 5) it follows that $N(21) \geq 4$, whereas $n(2) = \min(3, 7) - 1 = 2$. This provides the first counter example to MacNeish's conjecture. Similarly from symmetric $(s^2+s+1; s+1)$ with $s = 31$, we get $N(993) \geq 31$ whereas $n(993) = 2$.

We now prove,

Lemma 2. Suppose there exists a set Σ of q-1 m.o.L.S. of order k, then we can construct a q x k (k-1) matrix P, whose elements are the symbols 1,2,..., k and such that (i) any ordered pair (i, j), $i \neq j$ occurs as a column exactly once in any two rowed sub-matrix of P, (ii) P can be sub-divided into k-1 sub-matrices $P_1, P_2, \ldots, P_{k-1}$ of order q x k such that in each row of P_c, $1 \leq c \leq k-1$, each of the symbols 1, 2, ..., k occurs exactly once.

Proof: Without loss of generality take Σ in the standard form in which the first row of each Latin Square contains the symbols 1,2, ..., k in that order and prefix to the set Σ a square containing the symbol i in each position in the ith column. If we write down the elements of each square in a single row such that the symbol in the ith row and jth column occupies the nth position in the row, where $n = k(i-1) + j$, and from the resulting matrix, delete the first k

columns, then the resulting matrix P has the required properties (i) and (ii).

Let δ be a column of k distinct symbols $t_1, t_2, \ldots, t_k$. We denote by $P(\delta)$ the $q \times k(k-1)$ matrix obtained by replacing the symbol i by the treatment occurring in the ith position in δ. A similar meaning is assigned to $P_i(\delta)$ and $\pi_{c_j}(\delta)$ where π_{c_j} denotes the jth column of P_c. Clearly every treatment of δ occurs once in every row of $P_c(\delta)$, $c = 1,2,\ldots, k-1$, and if t_a and t_b are any two elementsof δ then the ordered pair (t_a, t_b) occurs as a column exactly once in any two-rowed sub-matrix of $P(\delta)$.

Theorem 2. Let there exist a pairwise balanced design (D) of index unity and type $(v; k_1, \ldots, k_m)$ and suppose that there exist $q_i - 1$ m.o.L.S. of order k_i. If

$$q = \min (q_1, q_2, \ldots, q_m)$$

then $N(v) \geq q-2$. If the design (D) is separable then $N(v) \geq q-1$.

Proof: Let the treatments of the design be $t_1, t_2, \ldots, t_v$ and let the blocks of the design (written out as columns) belonging to the equiblock component (D_i) be $\delta_{i_1}, \ldots, \delta_{i_{b_i}}$ $(i = 1,2,\ldots, m)$. Define the $k_i \times b_i$ matrix D_i by

$$D_i = [\delta_{i_1}, \ldots, \delta_{i_{b_i}}].$$

Let P_i be the matrix of order $q_i \times k_i (k_i - 1)$ defined in Lemma 2, the elements of P_i being the symbols $1, 2, \ldots, k_i$. Let P_{i_c}, $c = 1,2,\ldots, k_i - 1$ be the sub-matrices of P_i, such that each row each row of P_{i_c} contains the symbols $1,2,\ldots, k_i$ exactly once. Let $\pi_{i_{c_j}}$ be the jth column of P_{i_c} and let $P_i(\delta_{i_u})$, $u = 1,2,\ldots, b_i$, be the matrix obtained from P_i and δ_{i_u} Put

$$P_i(D_i) = [P_i(\delta_{i_1}), \ldots, P_i(\delta_{i_{b_i}})].$$

Then $P_i(D_i)$ is of order $q_i \times b_i k_i(k_i-1)$. If t_a and t_b are any two treatments occurring in the same block of (D_i) then the ordered pair (t_a, t_b) occurs exactly once as a column in any two-rowed submatrix of $P_i(D_i)$. Let Δ_i be the matrix obtained from $P_i(D_i)$ by retaining only the first q rows and let

$$\Delta = (\Delta_1, \Delta_2, \ldots, \Delta_m).$$

Then Δ is of order $q \times v(v-1)$ and it follows from the properties of the design that any two-rowed submatrix of Δ contains as a column each ordered pair of two distinct treatments chosen from $t_1, t_2, \ldots, t_v$ exactly once. This property of Δ will be referred to as property τ_2.

Let Δ_0 be a $q \times v$ matrix whose ith column contains t_i in every position, $i = 1, 2, \ldots, v$. Then the matrix $[\Delta_0, \Delta]$ is an orthogonal array $[v^2, q, v, 2]$. Hence $N(v) \geq q-2$.

To prove the second part consider each (D_i). Then since (D) is separable, each (D_i) can be broken up into sets $(D_{i_1}), \ldots, (D_{i_{r_i}})$ of type I (which we can take without loss of generality in the standard form) and sets $(D^*_{i_1}) \ldots (D^*_{i_{s_i}})$ of type II. Then obviously $P_i(D_i)$ can be separated into $k_i(k_i-1)$ sets with v columns each, such that each set has the property τ_1, that each row of every set contains the symbols $1, 2, \ldots, v$ exactly once. Also $P_i = (\ldots, P_{i_c} \ldots)$ $c = 1,2, \ldots, k-1$, where each P_{i_c} contains all the k_i symbols exactly once. Hence $P_{i_c}(D^*_{i_g})$ which contains v columns has also the property τ_2 $c = 1,2, \ldots, k-1$; $g = 1,2, \ldots, s_i$. It is now obvious that

$$P_i(D_i) = [P_i(D_{if}), \ldots, P_i(D^*_{ig}) \ldots]$$

$f = 1,2, \ldots, r_i$; $g = 1,2, \ldots, s_i$, possesses the property τ_1. If Δ_i has the same meaning as before, it is obvious that

$$\Delta = [\Delta_1, \ldots, \Delta_m] = [\Delta^{(1)}, \ldots, \Delta^{(v-1)}]$$

where each $\Delta^{(i)}$ the property τ_1. Defining Δ_o as before the matrix

$$(\Delta_o, \Delta)$$

also has the property τ_1. If α_i denotes a $1 \times v$ row vector each element of which is i, the matrix

$$\begin{pmatrix} \alpha_v & \alpha_1, \ldots, \alpha_{v-1} \\ \Delta_o & \Delta^{(1)}, \ldots, \Delta^{(v-1)} \end{pmatrix}$$

is an orthogonal array $[v^2, q+1, v, 2]$, which implies that $N(v) \geq q-1$.

Corollary: If b.i.b.d. $(v; k)$ exists, then $N(v) \geq N(k)-1$, and if the design is separable $N(v) \geq N(k)$.

It is known that resolvable solution to the b.i.b.d. $v = S^3+1$, $b = S^2(S^2-S+1)$, $r = S^2$, $k = S+1$, $\lambda = 1$ always exists for S a prime-power. Hence we have for $S = 31$.

Example 2. $N(31^3+1) = N(29792) \geq 31$, where as $n(29792) = 18$.

Similarly it is known that a resolvable solution to the b.i.b.d. with

$$v = S(S-1)/2, \; b = S^2-1, \; r = S+1, \; k = S/2 = 2^{m-1}, \; \lambda = 1$$

always exists. Hence taking $k = 8$, we have

Example 3. $N(120) \geq 7$, whereas $n(120) = 2$.

Theorem 3. Let there exist a design (D) of index unity and type $(v, k_1, k_2, \ldots, k_m)$ such that the set of equiblock components (D_1), (D_2), ..., (D_e), $e < m$, is a clear set. If there exist q_i-1 m.o.L.S. of order k_i, and if

$$q^* = \min (q_1+1, \ldots, q_e+1, q_{e+1}, \ldots, q_m)$$

then

$$N(v) \geq q^* - 2.$$

Proof: Define

$$q^{(1)} = \min (q_1+1, \ldots, q_e+1)$$

and

$$q^{(2)} = \min (q_{e+1}, \ldots, q_m)$$

Then

$$q^* = \min (q^{(1)}, q^{(2)})$$

Let $\delta_{i1}, \ldots, \delta_{ib_i}$ be the blocks of the component (D_i) written out as columns, $i \leq e$. There exist $q_i - 1$ m.o.L.S. of order k_i. Hence we can construct a orthogonal array A_{ij} with q_i+1 rows and k_i^2 columns whose symbols are the treatments occurring in δ_{ij}. Let

$$A_i = [A_{i1}, \ldots, A_{ib_i}].$$

Let Δ_i be the $q^* \times b_i k_i^2$ matrix obtained from A_i by retaining only the first q^* rows, and let

$$\Delta^{(1)} = [\Delta_1, \Delta_2, \ldots, \Delta_e].$$

Then $\Delta^{(1)}$ has q^* rows and $\sum b_i k_i^2$ columns. Clearly $\Delta^{(1)}$ has the property that if t_c and t_d are any two treatments identical or distinct occurring in any block of $(D_1), \ldots, (D_e)$, then the ordered pair (t_c, t_d) occurs as a column exactly once in any two-rowed sub-matrix of $\Delta^{(1)}$.

Consider the matrix P_i of order $q_i \times k_i(k_i-1)$ defined in Theorem 2, for $i = e+1, \ldots, m$ and let Δ_i be the matrix obtained from $P_i(D_i)$ by retaining only the first q^* rows. Then

$$\Delta^{(2)} = [\Delta_{e+1}, \Delta_{e+2}, \ldots, \Delta_m]$$

has the property that if t_a and t_b are any two distinct treatments contained in any block of $(D_{e+1}), \ldots, (D_m)$, then the ordered pair

(t_a, t_b) occurs exactly once in any two-rowed sub-matrix of $\Delta^{(2)}$. The number of columns in $\Delta^{(2)}$ is $\sum_{i=+1}^{m} b_i k_i(k_i-1)$. Again let $\Delta^{(3)}$ be the $q^* \times v_2$ matrix whose nth column contains t_n in every position, where t_n is any one of the $v_2 = v - \sum b_i k_i$ treatments not contained in $(D_1), \ldots, (D_e)$. Then $[\Delta^{(1)}, \Delta^{(2)}, \Delta^{(3)}]$ is an orthogonal array $[v^2, q^*, v, 2]$. Hence $N(v) \geq q^*-2$.

It is known that for a b.i.b.d. of the type $(v; 5)$, v must be of the form $20t+1$ or $20t+5$. A large number of designs of this type are known to exist. By omitting 3 treatments not occurring in the same block of such a design we have a large number of designs $(v-3; 5, 4, 3)$ from Example 2 of the last lecture, where the 3 blocks of size 3 form a clear set. Now $v-3$ is of the form $20t-2$ or $20t+2$, each of which is congruent to 2 mod. 4. Hence by applying the previous theorem we at once get many counter examples to Euler's conjecture.

Corollary 1. If $(20t+5; 5)$ exists then $N(20t+2) \geq 2$ and if $(20t+1; 5)$ exists then $N(20t-2) \geq 2$.

Example 4. Taking $t = 1$, in the above corollary, we have $N(22) \geq 2$, $N(18) \geq 2$.

Taking $t = 4$ in Example 1 of the previous lecture we know that a resolvable solution to the design $(24m+15; 3)$ with $r = 12m+7$ always exists. Adding a new treatment θ_i to all the blocks of the ith replication and adding a new block containing $\theta_1, \ldots, \theta_r$, we get a design of the type $(36m+22; 12m+7, 4)$ in which the single block of size $12m+7$ forms a clear set. Hence in the notation of the previous theorem $q_1=5$ since $N(12m+7) \geq n(12m+7) \geq 4$ and $q_2 = 4$. Therefore $q^*-2 = 2$. We therefore have

Corollary 2. $N(36m+22) \geq 2$ for every positive integer m.

Let v_1 be any number of the form $4t+2$ for which $n(v_1) \geq 2$ and let v_2 be any odd number. Then since $N(v_2) \geq 2$ from corollary 3 of Lemma 1 of the present lecture we have

Theorem 4. If there exist 2 m.o.L.S. of any order $4t+2$, then there exist at least 2 m.o.L.S. of any order which is an odd multiple of $4t+2$.

We can make use of this theorem in combination with Example 4 and Corollary 2 above to get an infinity of counter examples to Euler's conjecture.

Consider the finite projective plane $PG(2, 8)$. It can be shown that there exists on this plane a set $\sum$ of 10 points such that no three points of $\sum$ lie on a common line. Let $\sum^*$ be a subset of $\sum$. Then the number of points in $\sum^*$ is $x \leq 10$. Consider the set of retained points obtained by omitting the points of $\sum^*$. If we take the retained points as treatments and lines as blocks, then obviously we get a design of the type $(73-x; 7, 8, 9)$. Applying Theorem 2, we get

Example 5. If $x \leq 10$, $N(73-x) \geq 5$. In particular $N(70) \geq 5$, $N(66) \geq 5$ whereas $n(70) = n(66) = 1$.

Existence of a resolvable b.i.b.d. can be used to provide a number of pairwise balanced designs of index unity. If a resolvable $(v; k)$ exists with r as the number of replications, then we can construct

i) $(v+x; k, k+1, x)$ if $1 < x \leq r-2$

ii) $(v+r-1; k, k+1, r-1)$

iii) $(v+r; k, k+1, r)$

iv) $(v+1; k, k+1)$

where in (i) and (iii) the single blocks of size x and r restrictively form a clear set, and in (ii) the single block of size r and a replication of the original design form a clear set. Hence using Theorem 2 and Theorem 3 we have

Theorem 5. The existence of a resolvable (v, k) implies

i) $N(v+x) \geq \min (N(k), N(k+1), 1+N(x))-1$ if $1 < x \leq r-2$

ii) $N(v+r-1) \geq \min (N(k+1), 1+N(k), 1+N(r-1)) - 1$

iii) $N(v+r) \geq \min (N(k+1), 1+N(r)) - 1$

iv) $N(v+1) \geq \min (N(k), N(k+1)) - 1$

Example 6. From resolvable (49; 7), taking $x = 5$ we get $N(54) \geq 4$. Similarly from resolvable (21; 3) with $r = 10$, using (ii) above we get $N(30) \geq 2$.

Again consider a resolvable $(v; k)$ in which the blocks can be divided into n sets of type I. Then the number of replications is $r = kn$. Let the blocks be written as columns, and let (S_j) be the jth set of type I, the blocks being written in the standard form, $j = 1,2, \ldots, n$. Let us take r new treatments θ_{ij}, $i = 1,2,\ldots, k$; $j = 1,2, \ldots, n$. Define the $1 \times v$ row vector θ_{ij} with all elements θ_{ij}. Denote by

$$\begin{pmatrix} S_j \\ \theta_{ij} \end{pmatrix}$$

the result of adding θ_{ij} in the $(k+1)$th position to each block of (S_j).

Let $N(k+1) = q^{(1)}-1$. Then we can construct a $q^{(1)} \times (k+1)k$ matrix $P^{(1)} = (P_1^{(1)}, \ldots, P_k^{(1)})$ of Lemma 2. If δ_{ju} is the uth block of (S_j), $u = 1, 2, \ldots, v$; then the corresponding block of

$$\begin{pmatrix} S_j \\ \theta_{ij} \end{pmatrix}$$

is

$$\begin{pmatrix} \delta_{ju} \\ \theta_{ij} \end{pmatrix}$$

Consistent with our notation we denote by

$$P_i^{(1)} \quad \begin{pmatrix} \delta_{ju} \\ \theta_{ij} \end{pmatrix}$$

the result of replacing the symbols $1, 2, \ldots, k+1$ in $P_i^{(1)}$ by treatments in 1st, 2nd,..., $(k+1)$th position in

$$\begin{pmatrix} \delta_{ju} \\ \theta_{ij} \end{pmatrix}$$

and define

$$P_i^{(1)} \begin{pmatrix} S_j \\ \theta_{ij} \end{pmatrix} = [P_i^{(1)} \begin{pmatrix} \delta_{j1} \\ \theta_{ij} \end{pmatrix} \quad \ldots, \quad P_i^{(1)} \begin{pmatrix} \delta_{jv} \\ \theta_{ij} \end{pmatrix}]$$

A pair of distinct treatments belonging to (v; k) may be called a pure pair. Again a pair of treatments, one of which belongs to the original (v; k), and the other to the new added treatment, may be called a mixed pair. Then

$$\Delta_1 = [\ldots, P_i^{(1)} \begin{pmatrix} S_j \\ \theta_{ij} \end{pmatrix}, \ldots], \quad i = 1,2,\ldots, k; \; j = 1,2,\ldots,n;$$

has the property that any two-rowed sub-matrix contains as a column each pure and each mixed ordered pair of treatments exactly once.

Again if $q^{(2)} - 1 = N(r)$, we can form an orthogonal array $\Delta_2 = [r^2, q^{(2)} + 1, r, 2]$ whose symbols are the r new treatments. Let

$$q = \min (q^{(1)}, q^{(2)} + 1)$$

and let $\Delta^{(1)}$ and $\Delta^{(2)}$ be obtained from Δ_1 and Δ_2 by retaining only the first q rows. Also let $\Delta^{(3)}$ be the q x v matrix whose uth column contains the uth treatment of (v; k) in each position. Then

$$\Delta = [\Delta^{(1)}, \Delta^{(2)}, \Delta^{(3)}]$$

is an orthogonal array $[(v+r)^2, q, (v+r), 2]$. Hence we have

Theorem 6. If there exists a resolvable (v; k) with r replications, in which the blocks can be sub-divided into sets of type I, then

$$N(v+r) \geq \min (N(k+1), 1+N(r)) - 1$$

Example 7. From symmetric (7; 3) and (57; 8) we get $N(10) \geq 2$ and $N(65) \geq 7$.

We give below a simple proof by Dr. P.Keshava Menon of a theorem due to Bose, Shrinkhande and Parker.

Theorem 7. If $N(m) \geq 2$, then $N(3m+1) \geq 2$.

Proof: Let A be a circulant of order $2m+1$ in the integers $0,1,2, \ldots, 2m$.

$$A = \begin{pmatrix} 0 & 1 & 2 & \ldots & 2m \\ 2m & 0 & 1 & \ldots & 2m-1 \\ \ldots & & \ldots & & \ldots \\ 1 & 2 & 3 & \ldots & 0 \end{pmatrix}$$

Let B be a square matrix of order $2m+1$ whose first $m+1$ diagonals (counted from the principal diagonal onwards from left to right) are respectively the 1st $m+1$ rows of A and whose remaining m diagonals have the constant elements $2m+1, 2m+2, \ldots, 3m$ respectively.

$$B = \begin{pmatrix} 0 & 2m & 2m-1 & 2m-2 & 3m-1 & 3m \\ 3m & 1 & 0 & 2m & 3m-2 & 3m-1 \\ 3m-1 & 3m & 2 & 1 & & \\ \ldots & & \ldots & & \ldots & \ldots \\ 2m-3 & & & & 2m-1 & 2m-2 \\ 2m-1 & & & & 3m & 2m \end{pmatrix}$$

Let C be the matrix of order $(2m+1) \times m$ whose columns are the first m columns of A written from the bottom upwards

$$C = \begin{pmatrix} 1 & 2 & \ldots & m \\ 2 & 3 & \ldots & m+1 \\ \ldots & \ldots & \ldots & \ldots \\ 2m & 0 & \ldots & m-2 \\ 0 & 1 & \ldots & m-1 \end{pmatrix}$$

Let D be the matrix of order m x (2m+1) formed by the rows of A beginning with 2, 4,..., 2m respectively.

$$D = \begin{pmatrix} 2 & 3 & \cdots & 0 & 1 \\ 4 & 5 & \cdots & 2 & 3 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 2m & 0 & \cdots & 2m-2 & 2m-1 \end{pmatrix}$$

Finally let L_1 and L_2 be two m.o.L.S. of order m in the symbols 2m+1,..., 3m. Then

$$M_1 = \begin{pmatrix} B & C \\ D & L_1 \end{pmatrix} \qquad M_2 = \begin{pmatrix} B' & D' \\ C' & L_2 \end{pmatrix}$$

are two m.o.L.S. of order 3m+1, where B', C', and D' are the transposes of the corresponding matrices. The verification is left to the reader.

Taking $m = 4t+3$, we have $N(4t+3) \geq 2$ and hence

Corollary: $N(12t + 10) \geq 2$.

Example 8. Two superposed 10 x 10 orthogonal squares obtained by this method are given below, where the first (second) entries in each cell give the first (second) Latin Square:

00	69	58	47	71	83	95	12	24	36
96	11	09	68	57	72	84	23	35	40
85	90	22	19	08	67	73	34	46	51
74	86	91	33	29	18	07	45	50	62
17	75	80	92	44	39	28	56	61	03
38	27	76	81	93	55	49	60	02	14
59	48	37	70	82	94	66	01	13	25
21	32	43	54	65	06	10	77	88	99
42	53	64	05	16	20	31	89	97	78
63	04	15	26	30	41	52	98	79	87

Analogous to Theorem 5, we have the following theorem, the proof of which is omitted.

Theorem 8. Suppose there exists a resolvable GD $(v; k, m; 0, 1)$ with replications, then

i) $N(v+1) \geq \min (N(k), N(k+1), 1+N(m)) - 1$

ii) $N(v+x) \geq \min (N(k), N(k+1), 1+N(m), 1+N(x)) - 1$ if $1 < x < r$

iii) (a) $N(v+r) \geq \min (N(k+1), 1+N(m), 1+N(r)) - 1$

(b) $N(v+r) \geq \min (N(k+1), 1+N(k), 1+N(r), N(m+1)) - 1$

iv) $N(v+r+1) \geq \min (N(k+1), N(m+1), 1+N(r+1)) - 1$

where in part (iii) we choose whichever lower bound is better.

Combining this theorem with the Theorem 3 of the previous lecture, we have

Theorem 9. If $k \leq N(m)+1$, then

i) $N(km+1) \geq \min (N(k), N(k+1), 1+N(m)) - 1$

ii) $N(km+x) \geq \min (N(k), N(k+1), 1+N(m), 1+N(x)) - 1$ if $1 < x < m$.

Making use of the above theorems in conjunction with the existence of b.i.b.d. and group divisible designs, it is possible to prove that $N(v) \geq 2$ for $6 < v \leq 726$ excepting for $v = 14$ and 26. It is possible to prove by the method of differences that $N(14)$ and $N(26)$ are both ≥ 2. Thus $N(v) \geq 2$ for all v, $6 < v \leq 726$. Making use of this fact, we prove

Theorem 10. There exist at least two m.o.L.S. of any order $v > 6$.

Proof. It is sufficient to prove the theorem for $v = 2 \bmod 4$. $v \geq 730$. If v satisfies these conditions, then

$$v-10 = 144t + 4u, \quad t \geq 5, \quad 0 \leq u \leq 35$$

Hence

$$v = 4(36t) + 4u + 10$$

Since the least factor in the prime power decomposition of $36t$ is greater than or equal to 4, $N(36t) \geq 3$. Hence putting $k = 4$, $m = 36t$, $x = 4u + 10$, we have $k \leq 1 + N(m)$. Also $10 \leq x \leq 150$, $m \geq 180$. Hence $1 < x < m$ and $N(x) \geq 2$. Using the above theorem we get $N(v) \geq 2$.

Further reading

The following papers contain a large number of references.

1. R.C. Bose and S.S.Shrikhande: On the falsity of Euler's conjecture about the non-existence of two mutually orthogonal Latin Squares of order 4t+2, Proc. Nat. Acad. Sci., U.S.A. 45 (1959), 734-737.

2. --------- On the construction of sets of mutually orthogonal Latin Squares and the falsity of Euler's conjecture, Tran. Amer. Math. Soc. (1960), 191-209.

3. R. C. Bose, S.S.Shrinkhande and E.T.Parker : Further results on the construction of mutually orthogonal Latin Squares and the falsity of Euler's conjecture. Can. J. Math. 12 (1960), 189-203.

Minimum distance codes

1. Let S be any finite set. Denote by U_S its power set, i.e. the class of all subsets of S. Given A and B in U_S, we define their distance by

$$\delta(A, B) = N[(A \cup B) - (A \cap B)]/2$$

where $N(E)$ denotes the number of elements in E. It is easily verified that the distance satisfies all the postulates of a metric i.e. (i) $\delta(A, B) \geq 0$ and $= 0$ if and only if $A = B$, (ii) $\delta(A, B) = \delta(B, A)$, (iii) $\delta(A, B) \leq \delta(A, C) + \delta(C, B)$ for all A, B, C in U_S.

Given the sets $S_1, \ldots, S_k$, denote by

$$\pi S_i = S_1 \times S_2 \times \ldots \times S_k = [(s_1, s_2, \ldots, s_k),\ s_i \in S_i]$$

their cartesian product of ordered k-tuples. By identifying the element $(s_1, \ldots, s_k)$ with the set $[(1, s_1), (2, s_2), \ldots, (k, s_k)]$, πS_i may be regarded as a sub-class of an appropriate power set, the above definition yields a metric for cartesian products which states that for x, y in πS_i, $x = (x_1, \ldots, x_k)$, $y = (y_1, \ldots, y_k)$, $\delta(x, y)$ is the number of subscripts i for which $x_i \neq y_i$, $i = 1, 2, \ldots, k$.

2. Let C_n be the class of all n-place binary sequences in symbols 0 and 1. If $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are two sequences in C_n, define $x + y = (\ldots x_i + y_i, \ldots)$ where the sum is reduced mod. 2. Then C_n forms a Abelian Group of order 2^n. The null sequence is the identity of the group and every sequence is its own inverse. Define the weight (norm) of x, written as $W(x)$, as the number of unities in its representation. The number of places in which x and y differ is a distance between them and is called the Hamming distance. We can easily prove the following properties.

i) $\delta(x, y) = W(x + y)$

ii) $W(x + y) = W(x) + W(y) - 2(x.y)$

where $(x.y)$ denotes the scalar product of the two vectors x and y and is the number of places simultaneously occupied by unity in both.

iii) $\delta(x, y) = \delta(x + \alpha, y + \alpha)$ for any α in C_n

iv) $| W(x) - W(y) | \leq W(x+y) \leq W(x) + W(y)$

v) $W(x+y) \leq \min [W(x) + W(y), 2n - W(x) - W(y)]$

where n is the number of places in both.

3. A subset of C_n such that for any two elements α and β in $(\alpha \neq \beta)$ of the subset $\delta(\alpha, \beta) \geq d$ will be called a code with minimum distance d. If the subset is a subgroup of C_n, it will be called a group code. We shall denote minimum distance code by $M(n, d)$ and group code by $G(n, d)$.

We shall denote by $C_{n,r}$ $(r < n)$ the sub-group of C_n obtained by adding $n-r$ zeroes to each element of C_r. The number of elements in any subset will be denoted by $[E]$. Thus $[C_r] = 2^r$.

Given a fixed element α and a subset E of C_n the set of elements $\alpha + \beta$, $\beta \in E$ shall be denoted by $E + \alpha$. It is obvious that if E is a code with minimum distance d, then so is $E + \alpha$. If E is written as a matrix with r columns, then any permutation of rows and columns of E is also a minimum distance code.

Theorem 1. $[M(n, d)] \leq 2^{n-d+1}$

Proof. Consider the sub-group $C_{n,d-1}$. If α, β, $\alpha \neq \beta$, belong to $C_{n,d-1}$, then $W(\alpha + \beta) \leq d-1$. For any m_1, m_2 in $M = M(n,d)$, $w(m_1 + \alpha + m_2 + \beta) \geq d - (d-1) = 1$. Hence $\delta(m_1 + \alpha, m_2 + \beta) \neq 0$ i.e. $m_1 + \alpha$ and $m_2 + \beta$ are different. Thus $M + \alpha$ and $M + \beta$ are disjoint.

Hence $[M]\, 2^{d-1} \leq 2^n$ whence the result.

Theorem 2. For $n > d > 2$

$$[G(n, d)] \leq 2^{n-d}$$

Proof. Consider any two elements α, β $(\alpha \neq \beta)$ of $C_{n,d}$. Then $W(\alpha + \beta) \leq d$. If $\alpha + \beta < d$, then $G+\alpha$ and $G + \beta$ are disjoint. If $W(\alpha + \beta) = d$ and $\alpha + \beta$ does not belong to G then for any g_1, g_2 in G, $g_1 + \alpha = g_2 + \beta$ implies $\alpha + \beta = g_1 + g_2$ which is in G. Hence again $G + \alpha$, $G + \beta$ are disjoint. Hence if the element

$$x = (\underbrace{1, 1, \ldots,}_{d} \underbrace{0, 0, \ldots, 0}_{n-d})$$

does not belong to G; all the sets $G + \alpha$, α in $C_{n,d}$ are disjoint and hence

$$[G] \leq 2^{n-d}$$

If x belongs to G, this by interchanging the first and last columns of G, we get a code G' with the same minimum distance and having the same number of elements. If x does not belong to G', the theorem is true. If x belongs to G' then G must contain

$$y = (\underbrace{0, 1, 1, \ldots, 1}_{d-1} \quad \underbrace{0, 0, \ldots, 0, 1}_{n-d-1})$$

But then x+y of weight 2 belongs to G. Since G contains the null sequence $(0, \ldots, 0)$, the distance of x+y from this is 2 which is a contradiction.

Theorem 3. If $n > d+r$, $d > 2r+2$, (r an integer), then

$$[G(n,d)] \leq 2^{n-(d+r)}$$

Proof. For any two elements α, $\beta(\alpha \neq \beta)$ of $C_{n,d+r}$ for which $\alpha+\beta$ does not belong to G, $G+\alpha$ and $G+\beta$ are disjoint. Suppose $\alpha+\beta$ is in G. Then $W(\alpha+\beta) \geq d$. Let E be the set of elements of $C_{n,d+r}$ of weight $\geq d$. Suppose G contains an element x of E, which can be taken without loss of generality in the form

$$x = (\underbrace{1 \text{ at least } d-1 \text{ one's}}_{d+r-1}, \underbrace{0\ 0 \ldots 0}_{n-d-r})$$

Let G' be the code obtained from G by interchanging the first and last columns. If $\alpha+\beta$ does not belong to G', then $G'+\alpha$ and $G'+\beta$ are disjoint and hence $G+\alpha$ for varying α are also disjoint. Now suppose that G' contains an element of E, then G must have either an element

$$y = (0, \underbrace{\text{at least d one's}}_{d+r-1}, \underbrace{0, 0, \ldots 1}_{n-d-r})$$

or an element z of the form

$$z = (0, \underbrace{\text{at least d-1 one's}}_{d+r-1}, \underbrace{0, 0, \ldots, 0, 1}_{n-d-r})$$

In any case from (iv) in Section 1, we have

$$\delta(x, y) \leq 1 + 2(d+r-1) - (d+d-1) = 2r$$

and

$$\delta(x, z) \leq 1 + 2(d+r-1) - (d-1+d-1) = 2r + 2$$

But this is a contradiction since x, y, z belong to G. The theorem now follows immediately.

Theorem 4. If d is an odd number and if $2d + 1 > n$ then

$$[M(n,d)] \leq \frac{2d+2}{2d+1-n}$$

Proof. Let the elements of M $\alpha_1, \ldots, \alpha_m$, $m = [M(n,d)]$ be written as $m \times n$ matrix and let k_j be the number of unities in the jth column. We then have [Solomon Berger]

$$n \operatorname{Var}(k_j) = m \sum k_j - \frac{(\sum k_j)^2}{n} - \sum_{i<i'} \delta(\alpha_i, \alpha_{i'})$$

when $j = 1, 2, \ldots, n$; $i < i' = 1, 2, \ldots, m$. Putting $A = \sum k_j$ we have $\sum \delta(\alpha_i, \alpha_{i'}) \leq mA - A^2/n$.

But since A lies between 0 and mn, we have

$$\sum \delta(\alpha_i, \alpha_{i'}) \leq \frac{m^2 n}{4}$$

Hence

$$\frac{m(m-1)}{2} d \leq \frac{m^2 n}{4}$$

or

$$m \leq \frac{2d}{2d - n}$$

if

$$2d > n.$$

If d is an odd number, let r and s be the number of α's with odd and even weights. The distance between any two numbers is even if both are of odd or even weight and is an odd number otherwise. Hence

$$[(r(r-1) + s(s-1)] (d+1) + 2rsd \leq \frac{m^2 n}{2}$$

$$\text{or } m(m-1)d + r^2 + s^2 - m \leq \frac{m^2 n}{2}$$

$$\text{or } m(m-1)d - m \leq \frac{m^2 n}{2} - (r^2 + s^2)$$

$$\leq \frac{m^2 n}{2} - \frac{m^2}{2}$$

Hence

$$m \leq \frac{2d + 2}{2d + 1 - n}$$

if $2d + 1 > n$

Corollary. For $d + 1 \leq n < 2d$

$$[M(n, d)] \leq \frac{2d}{2d-n}$$

and the equality is attained if and only if there exists a b.i.b.d. with parameters

$$v = \frac{n}{2d-n}, \; b = n, \; r = n-d, \; k = \frac{n - d}{2d-n}, \; \lambda = \frac{2n - 3d}{2}$$

Proof. The first part is already proved above. By putting

$$\bar{k} = A/n = \frac{\sum k_j}{n} \text{ and } \bar{\delta} = 2 \sum_{i < i'} \delta(\alpha_i, \alpha_{i'})/m(m-1)$$

in (1) we have

$$\delta = \frac{mn}{2(m-1)} - \frac{2n}{m(m-1)}\left[\left(\bar{k} - \frac{m}{2}\right)^2 + \text{Var}\,(k_j)\right].$$

Hence

$$\delta \leq \frac{mn}{2(m-1)}$$

and the equality is attained if and only if $k_1 = k_2 \ldots = k_m = \frac{m}{2}$. Again if $M(n, d)$ is a code with $[M(n, d)] = \frac{2d}{2d-n}$, then variance $(k_j)=0$ and $d = \frac{mn}{2(m-1)}$. Hence $\delta(\alpha_i, \alpha_{i'}) \geq d$ and $\delta = d$ implies $\delta(\alpha_i, \alpha_i') = d = \frac{mn}{2(m-1)}$. Without loss of generality we can take the first row of M to consist entirely of unities. Then in the matrix M_1 of order $m-1 \times n$ every column contains exactly $\frac{m}{2} - 1$ unities and since the distance between any row of M_1 and the first row of M is $\frac{mn}{2(m-1)}$, every row of M_1 contains exactly $d = \frac{mn}{2(m-1)}$ zeroes and hence $n-d$ unities. Further the distance between any two rows of M_1 is d which implies that the number of places simultaneously occupied by unity in any two rows is $\frac{2n - 3d}{2}$. Thus M_1 is the incidence matrix of a b.i.b.d. with parameters.

$$v = \frac{n}{2d-n}, \quad b = n, \quad r = n-d, \quad k = \frac{n-d}{2d-r} \quad \lambda = \frac{2n-3d}{2}.$$

Conversely given the b.i.b. design by retraining the steps we can form M_1 and hence M which provides $M(n, d)$ with the maximum number of rows.

Example 1. Take $n = 4t-1$, $d = 2t$, we get the result that the existence of a symmetric b.i.b.d. with $v = 4t-1$, $k = 2t-1$, $\lambda = t-1$, is equivalent to the maximal set $M(4t-1, 2t)$ with $4t$ rows.

Theorem 5. If $[M(n, 2k-1)]$ and $[M(n+1, 2k)]$ represent the maximum number in the corresponding sets then

$$[M(n, 2k-1)] = [M(n+1, 2k)]$$

Proof. Every set $M(n+1, 2k)$ gives by omitting a column a set $M(n, 2k-1)$ with the same number of elements. Again in $M(n, 2k-1)$ if α and β are two elements both with odd or even weight, the distance between them (which is necessarily even) must be $\geq 2k$. Hence by adding a new component 0 to all elements of even weight and unity to all elements of odd weight, we get a set $M(n+1, 2k)$ with the same number of elements. The proof now follows immediately.

Exercise 1. Prove that

$$[M(n,d)] \leq 2[M(n-1, d)]$$

$$[M(2n, 2d)] \geq [M(n, 2d)][M(n, d)]$$

Exercise 2. Prove that for any integer t

i) $M(4t - 2, 2t) \leq 2t$

ii) $M(4t-1, 2t) \leq 4t$

iii) $M(4t, 2t) \leq 8t$

Further if the equality holds in (iii), then it also holds in (i) and (ii)

Theorem 6. The following statements are equivalent

(a) $M(4t, 2t) = 8t$

(b) $M(4t - 1, 2t) = 4t$

(c) b.i.b.d. $v = b = 4t-1$, $r = k = 2t - 1$, $\lambda = t-1$ exists

(d) A Hadamard matrix H_{4t} of order $4t$ exists.

Proof. In example 1. we have shown that (b) --> (c). Todd has shown that (c) --> (d). Hence (b), (c) and (d) are equivalent statements. We now show that (a) --> (b). Consider the set $M(4t, 2t)$ with $8t$ rows. Then in every column of this set both zero and unity occur exactly $4t$ times. For otherwise there is a column with $4t+i$ rows with unity or zero, $i > 0$. Retaining only these rows and omitting this column we get $[M(4t-1, 2t)] \geq 4t+i$ which contradicts the result in Exercise 2. Hence every column contains exactly $4t$ zero and $4t$

unities. Hence omitting a column and retaining rows with zeroes (or unities) alone, we get a set $M(4t-1, 2t)$ with $4t$ rows. Thus (a) --> (b). Since (b) <--> (d) it is sufficient to prove that (d) --> (a). Let H_{4t} be a Hadamard matrix with the initial row consisting entirely of unities and $\underline{H}_{4t}$ be obtained from H_{4t} by interchanging 1 and -1. Then replacing -1 by 0 in H_{4t} and $\underline{H}_{4t}$ we get H^*_{4t} and $\underline{H}^*_{4t}$. It is now easy to verify that the matrix

$$\begin{pmatrix} H^*_{4t} \\ \underline{H}^*_{4t} \end{pmatrix}$$

is a matrix in 0 and 1 with $8t$ rows and $4t$ columns such that the distance between any two rows is either $2t$ or $4t$. We thus have $M(4t, 2t)$ with $8t$ rows.

Lemma 1. For any real numbers $a_1, a_2, \ldots, a_n$

$$n\binom{a}{2} \leq \sum \binom{a_i}{2}$$

where $a = \dfrac{\sum a_i}{n}$ and $\binom{a}{2} = a(a-1)/2$

Proof of this lemma is omitted.

Definition. Let E be a class of subsets of any given set S. Then the t-extent of E, $e(E,t)$ is the greatest integer m such that E contains m distinct members having mutual distance greater than t.

Given this set $S(b)$ of b elements, let E_r denote the class of all subsets of $S(b)$ containing r elements. We prove the following

Theorem 7. If $r^2 - \lambda b > 0$ (λ integral and $0 \leq \lambda \leq r$), then

(a) $e(E_r, r - \lambda - 1) \leq v$ where $v = b(r-\lambda)/(r^2 - \lambda b)$

(b) Equality holds if and only if there exist v elements in E_r, such that $\delta(x_i, x_j) = r-\lambda$, for all $i \neq j = 1,2,\ldots,v$.

Proof. Let $e(E_r, r - \lambda - 1) = m$. Then since λ is integral there exist $x_1, x_2, \ldots, x_m$ in E_r such that $\delta(m_i, x_i) \geq r-\lambda$ for all $i \neq j$. Denote by k_i the number of sets x_i containing the ith

element of $S(b)$, $i = 1, 2, \ldots, b$. Comparing total occurrences we have

$$\text{(i)} \qquad \sum_{1}^{b} k_i = rm$$

and considering constributions to all set intersection, $\binom{m}{2}$ in number we have

$$\text{(ii)} \qquad \sum_{f}^{b} \binom{k_f}{2} = \sum_{i<j=1}^{m} N(x_i \cap x_j) = \sum_{i<j} [r - \delta(x_i, x_j)]$$

But then $\delta(x_i, x_j) \geq r - \lambda$ implies

$$\text{(iii)} \qquad \sum \binom{k_f}{2} \leq \lambda \binom{m}{2}$$

Using Lemma 1, we have

$$\text{(iv)} \quad L = b \binom{rm/b}{2} \leq M = \sum \binom{k_f}{2} \leq R = \lambda \binom{m}{2} .$$

Simple calculation shows that $L \leq R$ implies $m \leq v$ if $r^2 - \lambda b > 0$ and the equality is attained if and only if $m = v$. Thus conclusion (a) follows. Finally if $m = v$, then from $L = M = R$ and (ii) it follows that

$$\sum_{i<j} [r - \delta(x_i, x_j)] = \lambda \binom{m}{2},$$

and thus $\delta(x_i, x_j) \geq r - \lambda$ implies $r - \delta(x_i, x_j) = \lambda$.

Hence $\delta(x_i, x_j) = r - \lambda$. This completes the proof of (b).

Corollary 1. For $0 < \lambda < r < b$, the configuration $x_1, \ldots, x_v$ is the dual of a b.i.b.d. with parameters b, v, k, r, λ, where $k = rv/b$. Conversely, given the b.i.b.d. and considering its dual configuration as a subspace of E_r, one obtains $e(E_r, r - \lambda - 1) = v$, $r^2 - \lambda b > 0$ and $v = b(r-\lambda)/(r^2-\lambda b)$

Proof. In the proof of the above theorem from $m = v$, we obtain $L = M$. Thus together with Lemma 1 gives $k = k_i = (rv/b)$. Thus

every element of $S(b)$ occurs in exactly k of the subsets $x_1,\ldots,x_v$. Further $\delta(x_i, x_j)$ for all $i \neq j$ implies that every pair of distinct sets intersect in exactly λ elements. Thus the first conclusion follows. Conversely given the b.i.b.d. and considering its dual configuration as a subspace of E_r, one obtains $e(E_r, r - \lambda - 1) \geq v$. Further from $0 < \lambda < r < b$ and the well known inequalities $rv = bk$, $\lambda(v-1) = r(k-1)$ it follows that $r^2 - \lambda b > 0$ and $v = b(r-\lambda)/(r^2-\lambda b)$. But then from conclusion (a) of the theorem $e(E_r, r - \lambda - 1) = v$.

In the previous theorem, considering a set S of n symbols and identifying the element $a_1, a_2, \ldots, a_r$ with the set $(1, a_1)\ldots(r, a_r)$, we have $b = rn$ symbols and the set E_r becomes the space $S^r(n)$, the r-fold cartesian product of S with itself. Putting $\lambda + 1 = k$, the condition $r^2 > \lambda b$ of the theorem becomes $r^2-(k-1)rn>0$ or $r > (k-1)n$. Hence we have

Theorem 8. If $r > (k-1)n$, (k integral, $2 \leq k$, $n > 1$) then

(a) $e(S^r(n), r - k) \leq v$, where $v = \dfrac{n[r - (k-1)]}{r - (k-1)n}$

(b) If equality holds in (a) there exist v elements $x_1,\ldots, x_v$ in $S^r(n)$ such that $\delta(x_i, x_j) = r - (k-1)$, for all $i \neq j$. In this event, each element of $S(n)$ occurs as a jth component of exactly $t = \dfrac{r - (k-1)}{r - (k-1)n}$ of the x's, $j = 1, 2,\ldots, r$. Further from $x_1,\ldots, x_v$ we can construct a b.i.b.d. with parameters $v' = v$, $b'=rn$, $k' = t$, $r' = r$, $\lambda' = k-1$.

It is obvious that the nr symbols occurring in $x_1,\ldots, x_v$ are such that they can be divided into r groups of n each (for each $i = 1, 2, \ldots r$ the corresponding group is $(i, a_1),\ldots,(i, a_n)$) such that no two members of the same group occur together in any x. Hence the b.i.b.d. which is its dual is such that the nr blocks are divided into r sets of n each such that no two blocks of the same set have an element in common. Thus the b.i.b.d. obtained is a resolvable

design. Conversely given such a b.i.b.d. we can construct v elements of $S^r(n)$ with mutual distance exceeding r-k and the elementary conditions on its parameters will imply that $r > (k-1)n$.

Further reading

1. D. D. Joshi: A note on upper bounds for minimum distance codes, Informatio and Control, 1 (1958), 289-295.

2. R. C. Bose and S. S. Shrikhande: A note on a result in the theory of code construction, Information and Control, 2 (1959), 183-193.

3. R. E. A. C. Paley: On orthogonal matrices, J. Math. and Phys., 12 (1933), 311 - 320.

4. R. Silverman: A metrisation for power-sets with application to combinatorial analysis, Can. J. Math. 10 (1960), 158-176.

Lecture 7

Error Correcting Group Codes

1. The theory of communications and the more general information theory are concerned with the transmission of pieces of information from one place to another. In all practical situations the means of transmission - the channel is subject to random disturbances so that there is a positive probability that the reporting mechanism at the output end will announce information which is different from the one which is transmitted. A central problem is to devise encoding - decoding schemes which will keep small the probability of such erroneous reporting and which will utilise as far as possible the full capacity of the channel.

We shall be concerned with one specific type of communication system. Each piece of information is encoded as a sequence of n binary digits 0 and 1. The digits are presented, one at a time, for transmission over a symmetric binary channel, in which the error of transmission is $p < \frac{1}{2}$, i.e. the probability of receiving 1(0) when 0(1) is transmitted is p. It is further assumed that the noise on the channel operates independently on each symbol that is presented for transmission. The capacity of the channel based on concepts of information theory for quantifying the transfer of information is defined by

$$C = 1 + p \log_2 p + q \log_2 q \text{ bits/symbol}$$

where $q = 1-p$.

2. Suppose we have a set of K messages for transmission. Each message is called a letter and the set of K messages will be called an alphabet. Each letter is defined uniquely by a sequence of n binary digits and is transmitted over the channel by presenting, in order, to the channel input, the defining sequence of ones and zeroes. Such an alphabet is called K-letter, n-place binary signalling alphabet.

At the output end is a detector to translate the received sequence.

The minimum value of n to satisfy the requirements of defining the letter is the smallest integer k such that $2^k \geq K$. With this $n = k$, the probability of correct transmission is q^k. In practical situations this is not large enough to be acceptable. The alternative is to introduce redundancy into the definition of the letter i.e. each letter now contains $n > k$ binary digits and it is hoped to utilise the additional digit positions to 'correct' errors in transmission.

Let B_n be the set of 2^n n-place binary sequences. It is known that B_n is a group with respect to vector addition modulo 2 of the sequences.

Binary encoder. A v letter n-place binary encoder E is a subset of B_n consisting of v n-place sequences $\alpha_1, \alpha_2, \ldots, \alpha_v$.

Binary decoder. A v letter n-place binary decoder D is a correspondence between the v sequences. $\alpha_1, \ldots, \alpha_v$ and v mutually disjoint sets $S_1, \ldots, S_v$ of B_n such that $\bigcup_1^v S_i = B_n$.

Binary code. A v letter n-place binary code C is the combination (E, D) of a v-letter n-place binary encoder E and u-place binary decoder D.

Suppose the source alphabet consists of v letters (messages), $A_1, \ldots, A_v$ when the code C is used to transmit, the sequence α_i will be transmitted if A_i is meant to be sent, $i = 1, 2, \ldots, v$ and at the output end the letter transmitted is taken to be A_j, if the received binary sequence is a member of set S_j, $j = 1, 2, \ldots, v$.

A binary decoder D is said to be a minimum distance decoder if for any sequence β of the set S_i

$$\delta(\alpha_i, \beta) \leq \delta(\alpha_j, \beta), \quad \text{for } i, j = 1, 2, \ldots, v$$

where $\delta(x, y)$ stands for the Hamming distance.

A t-error correcting code. A v letter n-place binary code C is said to be t-error correcting if the decoder D is a minimum dis-

distance decoder and for any n-place sequence β

$$\delta(\alpha_i, \beta) \leq t \Rightarrow \beta \in S_i, \quad i = 1, 2, \ldots, v.$$

Suppose α_i is transmitted through the channel and there is disturbance in t or less of the positions of α_i. Then α_i is transmitted as $\alpha_i + y = \beta$ where y is an n-place sequence of weight not greater than t. Hence $\delta(\alpha_i, \beta) \leq t$ and consequently β is an element of S_i and hence will be decoded as α_i. Thus the transmission will be correct.

For an n-place, v-letter binary code C, the rate of information transmittal is defined as

$$R = \frac{\log_2 v}{n} \text{ bits per symbol.}$$

R is also called the rate of transmission. If the alphabet contains 2^k letters, then this reduces to

$$R = C_1 = \frac{k}{n}.$$

The basic existence theorem for general codes was given by Shannon and was proved in considerable generality by Wolfowitz. Applying it to the case of binary symmetric channel, we have 'Given any fixed $C_1 = C - \delta (\delta > 0)$ and any fixed $\varepsilon > 0$, there exists a number N such that for $n > N$ there exists a code with rate of information transmission C_1 and which will decode it with an error probability per block of n symbols (per letter) $Q_1(n, k, p) < \varepsilon$. If $C_1 > C$, no such N exists'.

The proofs of the above theorem are not constructive.

3. Group alphabet. Slepian has organised search for desirable alphabets and corresponding detection schemes by considering n-place group alphabets, or, briefly (n, k)-alphabets. An (n, k) alphabet is a sub-group of order 2^k of the group B_n of all binary sequences under vector addition modulo 2.

Let the letters of this alphabet be

$$\alpha_o = I = (0, 0, \ldots, 0), \alpha_1, \alpha_2, \ldots, \alpha_v, \quad v = 2^k - 1.$$

The group B_n can be developed according to the alphabet and its cosets

$\beta_o = \alpha_o = I$	α_1	α_2	$\cdots$	α_{v-1}
β_1	$\alpha_1+\beta_1$	$\alpha_2+\beta_1$	$\cdots$	$\alpha_v+\beta_1$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
β_μ	$\alpha_1+\beta_\mu$	$\alpha_2+\beta_\mu$	$\cdots$	$\alpha_v+\beta_\mu$

where $\mu = 2^{n-k}-1$, and β_e is an n-place sequence which has not appeared in cosets led by $\beta_0, \beta_1, \ldots, \beta_{e-1}$. The elements β_e are called coset leaders.

Because of the group property, any coset is repeated with elements in a different order, if the coset leader is replaced by any other element of the coset. We agree to take β_e as that element (or any one of those elements) of the coset whose weight is the least. The detection scheme is then the following: if the element of B_n which is received at the output end lies in column i of the coset array, the detector prints the letter α_i. If the elements of B_n are written in the above form, then it is said to be represented in a standard array.

Example: B_4 can be developed according to the (4, 2) alphabet 0000, 1100, 0011, 1111 as follows:

0000	1100	0011	1111
1010	0110	1001	0101
1110	0010	1101	0001
1000	0100	1011	0111

This can be written in a standard form as follows:

0000	1100	0011	1111
1010	0110	1001	0101
0010	1110	0001	1101
1000	0100	1011	0111

For the original array, in the second row any number could be taken as a coset leader as all of them are of weight 2. Similarly in the third and fourth row each there are two possible ways of selecting the coset leader.

For such a code

$$Q_1 = P(\alpha_i \text{ is correctly produced by the detector})$$

$$= \sum_{j=0}^{\mu} P(\gamma_i + \beta_j / \alpha_i)$$

$$= \sum_j p^{w(\beta_j)} q^{n-w(\beta_j)}$$

since $p < \frac{1}{2}$, $p^w q^{n-w}$ is a monotonic decreasing function of w, one sees the motivation for taking β_j as the element of minimum weight. Slepian has shown that for the given alphabet no other detection scheme has a greater average probability that a transmitted letter is correctly produced by the decoder. Thus the proposed decoder is a maximum likelihood decoder.

An essential feature of the proposed (n, k) code is the following. When the letter α is transmitted, the decoder will correctly report α if and only if the channel produces the sequence $\alpha+\beta_j$, $j = 0, \ldots, \mu$, i.e. if and only if the errors in transmission occur in precisely those positions occupied by unity in a coset leader. Hence if all n-place sequences of weight s can serve as coset leaders, then the code will correct all s-tuple errors. If the number of coset leaders of weight s is less than $\binom{n}{s}$, say α, then the code will correct α s-tuple errors. The advantage of maximising the number of lowest weight sequences serving as coset leaders now appears again with respect to maximising the number W such that all errors of weight W or less are corrected by the code.

We now give some results due to Bose and Ray Chaudhuri.

Theorem 1. The necessary and sufficient condition for an (n, k) binary group code to be t-error correcting is that each letter of the alphabet except the null letter has weight 2t+1 or more.

Proof. Let $\alpha_0, \alpha_1, \ldots, \alpha_v$ be the letters of the alphabet. Let β be any n-place sequence for which $W(\beta) \leq t$. Then

$$\delta(\alpha_i, \beta) = W(\alpha_i+\beta) = W(\alpha_i) + W(\beta) - 2(\alpha_i.\beta)$$

But $W(\beta) \leq t$ implies $(\alpha_i.\beta) \leq t$. Hence

$$W(\alpha_i+\beta) - W(\beta) \geq W(\alpha_i) - 2t.$$

The necessary and sufficient condition for β to be the leader of the coset in which it occurs is that the left hand side of the above relation is a positive integer for $i = 1, \ldots, v$. Hence the theorem.

Since the $v+1 = 2^k$ messages can be transmitted by a k-place binary code if there is no error, the number $r = n-k$ is called the redundancy of the (n,k) binary group code. In constructing a t-error correcting (n, k) binary code for given n and t one would like to maximise k i.e. maximise the number of different messages that it is possible to transmit.

Theorem 2. The necessary and sufficient condition for the existence of a t-error correcting (n, k) binary group code is the existence of a matrix A of order n x r and rank $r = n-k$ with elements from GF(2), such that any set of 2t row vectors of A are independent.

Proof. We first prove the sufficiency. Suppose the matrix A has the property (P_{2t}) that any set of 2t rows are independent. Clearly $n > r \geq 2t$. The property (P_{2t}) remains invariant under the following operations: (i) interchange of any two rows or columns, (ii) replacement of the ith column by the sum of ith and jth column, $i \neq j$. By these operations A can be transformed to

$$A^* = \begin{pmatrix} I_r \\ C \end{pmatrix}$$

where A^* has the property (P_{2t}), I_r is the unit matrix of order r and C is a matrix of order $k \times r$. Consider the matrix

$$C^* = (C\ I_k).$$

Then C^* is of order $k \times n$. We show that the k rows of C^* are the generators (under vector addition modulo 2) of a group G of order 2^k such that if α is any arbitrary (non-null) vector of G, then $W(\alpha) \geq 2t+1$. Suppose α is dependent on some d rows of C^*, $d \leq k$, then α is the sum of these d rows. We can write $\alpha = (y\ \varepsilon)$ where y is the part coming from C and ε the part coming from I_k. Then $W(\alpha) = W(y) + W(\varepsilon) = W(y)+d$. Hence $W(\alpha) \geq 2t+1$ if $d \geq 2t+1$. Hence suppose $d \leq 2t$. If $W(\alpha) < 2t+1$, then $W(y) \leq 2t-d$. Let $W(y) = c$. There are exactly c positions in y which are occupied by unity. Corresponding to each such position we can find a row of I_r which has unity in this position and zero elsewhere. Then these c vectors of I_r together with the t rows of C whose sum is y, constitute a set of $c+d$ vectors which are dependent, for their sum is the null vector. But $c+d \leq 2t$, this contradicts the fact that A^* has property (P_{2t}). Thus the weight of any non-null sequence of G is greater than or equal to $2t+1$. From theorem 1, it follows that G forms a t-error correcting (n, k) group code.

To prove necessity, suppose there exists a t-error correcting (n, k) group code. Then by theorem 1, we can find a set of k n-place sequences with elements in GF(2), which under vector addition generate the group of sequences constituting the letters of the alphabet. If α is a sequence of this group then $W(\alpha) \geq 2t+1$. Let C^* of order $K \times n$ be the matrix which generates this group. If we interchange any two rows or columns of C^*, or replace the ith row of C^* by the sum of the ith and jth row ($i \neq j$), the transformed matrix still has the property that its rows generate a group with each sequence of weight greater than or equal to $2t+1$. Hence without loss of

generality we can take

$$C^* = (C\ I_k)$$

as above. By retracing the arguments used in proving sufficiency we see that the matrix

$$A^* = \begin{pmatrix} I_r \\ C \end{pmatrix}$$

has the property (P_{2t}). This completes the proof of necessity.

Corollary 1. The existence of a t-error correcting (n,k) group code implies the existence of a t-error correcting (n-c, k-c) group code when $0 < c < k$.

If in the matrix A with property (P_{2t}) we omit c rows, $0 < c < k$, then the resulting matrix of order $n-c \times r$ has the same property (P_{2t}). Hence the result.

Let V_r denote the vector space of all r-vectors whose elements belong to GF(2). Consider the maximum number of vectors in a set $\sum$ chosen from V_r, such that any 2t distinct vectors of $\sum$ are independent. This number may be denoted by $n_{2t}(r)$, and the problem of finding the set $\sum$ may be called the packing problem of order 2t for V_r. For a given t, it is obvious that $n_{2t}(r)$ is monotonic increasing function of r.

Let $k = k_t(n)$ denote the maximum value of k such that a t-error correcting (n, k) group code for given t and n exists. We then have

Theorem 3. If $n_{2t}(r) \geq n > n_{2t}(r-1)$, then $k_t(n) = n-r$.

Proof. By the previous theorem there exists a t-error correcting $(n_{2t}(r), n_{2t}(r)-r)$ binary group code. Hence from the lemma there exists a t-error correcting (n, n-r) group code. But a t-error correcting $(n_1, n-r+1)$ does not exist, for this would imply that $n_{2t}(r-1) \geq n$. Hence $k_t(n) = n-r$ is the maximum value of k for which a t-error correcting (n, k) group code exists.

Thus the problem of finding a t-error correcting (n,k) group code is equivalent to finding the smallest r for which there exists a set of n or more distinct vectors of V_r, such that any 2t distinct vectors from the set are independent.

Lemma 1. If $X_1, X_2, \ldots, X_e$ are different non-zero elements of $GF(2^m)$, then the equations

$$\sum_{j=1} x_j^{2_i-1} = 0, \quad i = 1,2, \ldots, t \tag{3.1}$$

cannot hold simultaneously if $e \leq 2t$.

Proof. Suppose the equations (3.1) hold simultaneously. Let

$$X^e + p_1 X^{e-1} + p_2 X^{e-1} + \ldots + p_e = 0 \tag{3.2}$$

be the algebraic equation with roots $X_1, \ldots, X_e$. Then p_j is in $GF(2^m)$ and is the sum of the products of the roots taken j at a time. Define S_j as the sum of the jth powers of the roots. For a field of characteristic 2, the well known relations between S_j and p_j become

$$\begin{aligned} &S_1 + \delta_1 p_1 = 0 \\ &S_2 + p_1 S_1 + \delta_2 p_2 = 0 \\ &\ldots \quad \ldots \quad \ldots \\ &S_e + p_1 S_{e-1} + \ldots + \delta_e p_e = 0 \end{aligned} \tag{3.3}$$

where $\delta_i = 0$ or 1 according as i is even or odd. From (3.1) $S_j = 0$ when j is odd ($j < 2t$). Then from (3.3) it follows that $S_j = 0$ if j is even ($j \leq e$) and $p_j = 0$ if j is odd ($j \leq e$).

Case (i). If e is odd, then $p_e = X_1 X_2, \ldots, X_e \neq 0$, since $X_1, X_2, \ldots, X_e$ are non-zero. Hence a contradiction.

Case (ii). If e is even, say $e = 2m$, then from (3.2)

$$x^{2m} + p_2 x^{2m-2} + \ldots + p_{2m} = 0 \tag{3.4}$$

Now each coefficient p_{2j} is some power α^c, where α is a primitive element of $GF(2^m)$ and hence $\alpha^{2m-1} = 1$. Using $\alpha^c = \alpha^{(2m-1)+c}$, it is obvious that each p_{2j} has a unique square root q_j. Hence we get

$$(X^m + q_1X^{m-1} + \ldots + q_m)^2 = 0 \qquad (3.5)$$

Thus (3.2) cannot have more than m distinct roots, which is again a contradiction, since $X_1, X_2, \ldots, X_e$ are all distinct.

The proof of the lemma is complete.

4. Let V_m be the vector space of m-vectors with elements from GF(2). Since each element of $GF(2^m)$ is of the form $a_o + a_1X + \ldots + a_mX^{m-1}$, where X is a given primitive element of the field, we can set up a one-to-one correspondence between the vector $\alpha = (a_o, a_1, \ldots a_m)$ and the element $a_o + a_1X + \ldots a_{m-1}X^{m-1}$ of $GF(2^m)$. In this correspondance the null vector of V_m corresponds to the zero of $GF(2^m)$ and the sum of any two vectors corresponds to the sum of the corresponding elements of $GF(2^m)$. This essentially defines the multiplication of two vectors and converts it into a field.

Let V_{mt} be the vector space of all mt-vectors with elements from GF(2). To any element α_i of V_m there corresponds a unique vector α_i^* of V_{mt} defined by

$$\alpha_i^* = (\alpha_i\ \alpha_i^3 \ldots, \alpha_i^{2t-1}) \qquad (4.1)$$

though the converse is not true.

There are $n = 2^m - 1$ distinct non-null vectors in V_m. Let

$$M^* = \begin{pmatrix} \alpha_1 & \alpha_1^3 & \ldots & \alpha_1^{2t-1} \\ \alpha_2 & \alpha_2^3 & \ldots & \alpha_2^{2t-1} \\ \ldots & \ldots & \ldots & \ldots \\ \alpha_n & \alpha_n^3 & \ldots & \alpha_n^{2t-1} \end{pmatrix} \qquad (4.2)$$

be the matrix, which has for row vectors the corresponding vectors $\alpha_1^*, \ldots, \alpha_n^*$. By the previous lemma, the sum of any e row vectors of M^*, $e \leq 2t$ is non-null. Hence replacing each element of M^* by the corresponding m-place binary vector, we see that M^* has the property (P_{2t}).

Now rank $(M^*) \leq mt$. Since there is essentially one Galois field $GF(2^m)$, this rank is a definite function of m and t which we denote by $R(m, t)$. If $R(m, t) < mt$, we can choose $R(m, t)$ independent columns of M^* and delete the remaining ones. The matrix A so obtained has still the property (P_{2t}). Hence from Theorem 2, we have

Theorem 4. If $n = 2^m-1$, we can obtain t-error correcting (n, k) binary group code where $k = 2^m-1-R(m, t) \geq 2^m-1-mt$.

Exercise. Construct a 3-error correcting (15, 5) group code by considering the minimal function $X^4 + X + 1$ to generate $GF(2^4)$.

Further reading

1. A. Feinstein : Foundations of information theory (1958). McGraw Hill.
2. A. Khinchin : Mathematical foundations of information theory, (1958). Dover Publications.
3. D. Slepian : A class of binary signalling alphabets, Bell System. Technical Journal, 35 (1956), 203-234.
4. R. C. Bose and D. K. Roychoudhari: On a class of error correcting binary group codes. Information and Control (1960).