DIFFERENCE SETS AND COMBINATORIAL ARRANGEMENTS DERIVABLE FROM FINITE GEOMETRIES.

By C. RADHAKRISHNA RAO.

(Communicated by S. N. Roy, M.Sc., F.N.I.)

(*Received July 17; Read November 19, 1945.*)

§0. INTRODUCTION.

In an earlier paper by the author (1945) a chain of theorems have been derived of the form, given an integer v, it is possible to find s sets of k integers each—

$$\left.\begin{array}{cccc} d_{11} & d_{21} & \ldots & d_{k1} \\ d_{12} & d_{22} & \ldots & d_{k2} \\ \ldots & \ldots & & \\ \ldots & \ldots & & \\ d_{1s} & d_{2s} & \ldots & d_{ks} \end{array}\right\} \qquad (0.10)$$

such that among the $sk(k-1)$ differences $d_{ir}-d_{jr}$ $(i, j = 1, 2, \ldots k\ ;\ i \neq j\ ;\ r = 1, 2, \ldots s)$ reduced modulo v contain all integers less than v and not divisible by θ, λ_1 times and those divisible by θ, λ_2 times. The value of v is either $(m^{t+1}-1)/(m-1)$ or (m^t-1) where $m = p^n$ (p being a prime) and θ either $(m^{t+1}-1)/(m^2-1)$ or $(m^t-1)/(m-1)$.

(2) These theorems have been derived with the help of a compact representation of finite geometries and two theorems which are termed as *theorems of differences*. Incidentally various results which are helpful in the actual derivation of the sets (0.10) which are known as *the difference sets* and the solution of combinatorial problems have been obtained.

(3) The object of the present paper is twofold. The first is to derive systematic and quicker methods of the derivation of difference sets and study the connection between finite geometries and the existence of such difference sets. The second is to study some general class of combinatorial problems and obtain solutions with the help of finite geometrical configurations and the number theory results derived from them.

(4) The main results of the paper are,

(*a*) the existence of difference sets does not imply that a suitable finite geometry ($PG(t, m)$ or $EG(t, m)$) exists,

(*b*) the actual derivation of the difference sets ultimately depends on the properties and solutions of certain recurrence relations,

(*c*) the existence of difference sets supplies a compact representation of the solutions to Incomplete balanced designs, and

(*d*) the finite geometrical configurations are helpful in constructing Latin Cubes and Hyper Cubes of a certain class useful in finding out confounded designs in the case of symmetrical and asymmetrical factorial experiments.

§1. Fields and Galois Arithmetics.

If a field contains m elements then it is represented by $GF(m)$. A set of polynomials $f(x)$ defined by $f(x) = a_0+a_1x+a_2x^2+ \ldots$ where $a_0, a_1, \ldots$ are elements of $GF(p)$ (the field formed by the residue classes mod p, a prime integer) are represented by $GF_p[x]$. The addition and multiplication are defined as in usual algebra with the only rule that the coefficients are reduced to (mod p) at the final stage.

(2) A polynomial $\theta(x)$ in $GF_p[x]$ is said to be irreducible when it is not possible to express it as the product of two polynomials belonging to $GF_p[x]$. Let us consider the residue classes mod $\theta(x)$, an irreducible polynomial of the n-th degree in $GF_p[x]$. There are evidently p^n residue classes which are capable of the standard representation

$$b_0+b_1x+ \ldots b_{n-1}x^{n-1} \tag{1.20}$$

where $b_0, b_1, \ldots$ run over the elements of $GF(p)$. These residue classes can be easily shown to form a field with p^n elements and is represented by $GF(p^n)$. A non-zero element of $GF(p^n)$ satisfies the equation $x^{p^n-1} = 1$ which may be considered as a generalisation of Fermat's theorem. If r is the least integer for which an element α satisfies the equation $\alpha^r=1$ then r is said to be the order of α. An element with the order p^n-1 is said to be a primitive element. By a suitable choice of $\theta(x)$ which is called the minimum function it is possible to get the residue class x as a primitive element in which case all the elements are represented by

$$0, x^0, x^1, \ldots x^{p^n-2} \tag{1.21}$$

which is called the power cycle of x, each of which is congruent to a polynomial of degree less than n. The process of multiplication is carried on with the elements (1.21) and the addition with the polynomial forms. Thus if $x^r \equiv a_0+a_1x+ \ldots a_{n-1}x^{n-1}$ and $x^s \equiv b_0+b_1x+ \ldots b_{n-1}x^{n-1}$ then $x^rx^s=x^{r+s}$ and $x^r+x^s = (a_0+b_0)+(a_1+b_1)x+ \ldots (a_{n-1}+b_{n-1})x^{n-1}$. These calculations are popularly termed as the Galois Arithmetics.

(3) The methods for constructing the minimum functions have been extensively studied by Bose, Chowla and Rao (1945) in the case of $GF(p^2)$ and similar studies are progressing for other cases. If

$$\theta(x) = a_0+a_1x+ \ldots a_nx^n \tag{1.30}$$

where $a_0, a_1, \ldots$ are elements of $GF(p)$, is a minimum function for $GF(p^n)$ then it has been shown that

$$x^w = (-)^na_0 \pmod{\theta(x)} \tag{1.31}$$

where $w = (p^n-1)/(p-1)$, so that knowing the power cycle up to x^{w-1} all the others can be constructed by multiplication with a_0 and its powers. Thus if $x^c = b_0+b_1x+ \ldots +b_{n-1}x^{n-1}$, then $(-1)^{nr}x^{c+wr} = a^r{}_0b_0+a^r{}_0b_1x+ \ldots +a^r{}_0b_{n-1}x^{n-1}$. In the following table of power cycles the congruent polynomials are recorded only for powers of x's up to w, the rest being easily derivable with the help of the constant in the minimum function as discussed above.

Table 1.

Power cycle for $GF(p^n)$.

p^n	Minimum function.	Power cycle.
2^2	x^2+x+1	$x^0 = 1, x = x, x^2 = x+1.$
2^3	x^3+x^2+1	$x^0 = 1, x = x, x^2 = x^2, x^3 = x^2+1, x^4 = x^2+x+1, x^5 = x+1, x^6 = x^2+x.$
3^2	x^2+x+2	$x^0 = 1, x = x, x^2 = 2x+1, x^3 = 2x+2, x^4 = 2.$
2^4	x^4+x^3+1	$x^0 = 1, x = x, x^2 = x^2, x^3 = x^3, x^4 = x^3+1, x^5 = x^3+x+1, x^6 = x^3+x^2+x+1, x^7 = x^2+x+1, x^8 = x^3+x^2+x, x^9 = x^2+1, x^{10} = x^3+x, x^{11} = x^3+x^2+1, x^{12} = x+1, x^{13} = x^2+x, x^{14} = x^3+x^2.$
5^2	x^2+2x+3	$x^0+1, x = x, x^2 = 3x+2, x^3 = x+1, x^4 = 4x+2, x^5 = 4x+3, x^6 = 3.$
3^3	x^3+2x+1	$x^0 = 1, x = x, x^2 = x^2, x^3 = x+2, x^4 = x^2+2x, x^5 = 2x^2+x+2, x^6 = x^2+x+1, x^7 = x^2+2x+2, x^8 = 2x^2+2, x^9 = x+1, x^{10} = x^2+x, x^{11} = x^2+x+2, x^{12} = x^2+2, x^{13} = 2.$

Power cycle for $GF(p^n)$.

p^n	Minimum function.	Power cycle.
2^5	x^5+x^2+1	$x^0=1, x=x, x^2=x^2, x^3=x^3, x^4=x^4, x^5=x^2+1, x^6=x^3+x, x^7=x^4+x^2, x^8=x^3+x^2+1, x^9=x^4+x^3+x, x^{10}=x^4+1, x^{11}=x^2+x+1, x^{12}=x^3+x^2+x, x^{13}=x^4+x^3+x^2, x^{14}=x^4+x^3+x^2+1, x^{15}=x^4+x^3+x^2+x+1, x^{16}=x^4+x^3+x+1, x^{17}=x^4+x+1, x^{18}=x+1, x^{19}=x^2+x, x^{20}=x^3+x^2, x^{21}=x^4+x^3, x^{22}=x^4+x^2+1, x^{23}=x^3+x^2+x+1, x^{24}=x^4+x^3+x^2+x, x^{25}=x^4+x^3+1, x^{26}=x^4+x^2+x+1, x^{27}=x^3+x+1, x^{28}=x^4+x^2+x, x^{29}=x^3+1, x^{30}=x^4+x.$
3^4	$x^4+x^3+x^2+2x+2.$	$x^0=1, x=x, x^2=x^2, x^3=x^3, x^4=2x^3+2x^2+x+1, x^5=2x^2+2, x^6=2x^3+2x, x^7=x^3+2x+2, x^8=2x^3+x^2+1, x^9=2x^3+x^2+2, x^{10}=2x^3+x^2+x+2, x^{11}=2x^3+2x^2+x+2, x^{12}=2x^2+x+2, x^{13}=2x^3+x^2+2x, x^{14}=2x^3+2x+1, x^{15}=x^3+x+2, x^{16}=2x^3+1, x^{17}=x^3+x^2+2, x^{18}=2x^2+1, x^{19}=2x^3+x, x^{20}=x^3+2x^2+2x+2, x^{21}=x^3+x^2+1, x^{22}=2x^2+2x+1, x^{23}=2x^3+2x^2+x, x^{24}=2x^2+2x+2, x^{25}=2x^3+2x^2+2x, x^{26}=2x+2, x^{27}=2x^2+2x, x^{28}=2x^3+2x^2, x^{29}=x^2+2x+2, x^{30}=x^3+2x^2+2x, x^{31}=x^3+x^2+x+1, x^{32}=2x+1, x^{33}=2x^2+x, x^{34}=2x^3+x^2, x^{35}=2x^3+x^2+2x+2, x^{36}=2x^3+x+2, x^{37}=x^3+2x^2+x+2, x^{38}=x^3+1, x^{39}=2x^3+2x^2+2x+1, x^{40}=2.$

§2. Finite Geometries and Difference Sets.

The points of $PG(t, m)$ (finite Projective Geometry of t dimensions with $(m+1)$ points on a line) are represented by the non-zero marks or elements of $GF(m^{t+1})$, two elements x^α and x^β (where x is a primitive element in $GF(m^{t+1})$) representing the same point if $x^\alpha = ax^\beta$, where a is an element of $GF(m)$. The $(d+1)$ distinct points represented by the elements x^{α_0}, x^{α_1}, . . . x^{α_d} with no linear relation among them with coefficients as the elements of $GF(m)$ constitute a d-flat whose equation is represented by $a_0x^{\alpha_0}+a_1x^{\alpha_1}+$ . . . $a_dx^{\alpha_d}$ where a's are elements of $GF(m)$. All the points lying on this flat are obtained by allowing a's to run through the elements of $GF(m)$, not all being simultaneously zero. We denote these $(m^{d+1}-1)/(m-1)$ elements representing the points on the above d-flat as

$$E[\Sigma a_i x^{\alpha_i},\ A\neq 0,\ \subset GF(m),\ X \subset GF(m^{t+1})] \tag{2.10}$$

and the powers of x's in the above reduced mod $(m^{t+1}-1)/(m-1)$ as $D[E, (2.10) \bmod (m^{t+1}-1)/(m-1)]$ in general or in particular as

$$D[\Sigma a_i x^{\alpha_i},\ A\neq 0,\ \subset GF(m),\ X \subset GF(m^{t+1}),\ \bmod\ (m^{t+1}-1)/(m-1)] \tag{2.11}$$

or when the context is clear (2.10) and (2.11) may be replaced by $E[\Sigma a_i x^{\alpha_i}]$ and $D[\Sigma a_i x^{\alpha_i}, \bmod (m^{t+1}-1)/(m-1)]$

(2) In the previous paper it has been shown that by suitably choosing some d-flats which are termed as initial flats and carrying on the operation D in (2.11) we get difference sets of a certain description. Starting with the difference set so constructed, we can arrive at all the d-flats in the geometry by a process of cyclical development. The question arises as to whether the existence of a difference set of the same description as above ensures the existence of the geometry $PG(t, m)$. It is easy to demonstrate that in the case of difference sets derived by considering lines in $PG(2, m)$ this converse property holds. But this need not be true of the difference sets of the theorem mentioned in the introduction.

(3) By considering lines in $PG(3, 2)$ we arrive at the difference sets

$$(0, 1, 4),\ (0, 2, 8) \tag{2.30}$$

of cycle 15 with the property that the differences arising from them (mod 15) contain all integers less than 15 and not divisible by 5 once each. To these we may add the set (0, 5, 10) of cycle 5 which on cyclical development generate the 35 lines in $PG(t, m)$. Let us consider the sets

$$(2, 5, 6),\ (0, 2, 8) \tag{2.31}$$

which possess the same properties as (2.30). By adding to this the set (0, 5, 10) of cycle 5 we can generate the following 35 lines.

$$\left.\begin{array}{lll} 2, 5, 6 & 14, 2, 3 & 9, 11, 2 \\ 3, 6, 7 & 0, 3, 4 & 10, 12, 3 \\ 4, 7, 8 & 1, 4, 5 & 11, 13, 4 \\ \hline 5, 8, 9 & 0, 2, 8 & 12, 14, 5 \\ 6, 9, 10 & 1, 3, 9 & 13, 0, 6 \\ 7, 10, 11 & 2, 4, 10 & 14, 1, 7 \\ \hline 8, 11, 12 & 3, 5, 11 & 0, 5, 10 \\ 9, 12, 13 & 4, 6, 12 & 1, 6, 11 \\ 10, 13, 14 & 5, 7, 13 & 2, 7, 12 \\ 11, 14, 0 & 6, 8, 14 & 3, 8, 13 \\ 12, 0, 1 & 7, 9, 0 & 4, 9, 14 \\ 13, 1, 2 & 8, 10, 1 & \end{array}\right\} \quad (2.32)$$

The lines (0, 5, 10), (0, 2, 8) and (2, 5, 6) intersect two by two. According to postulates of Veblen and Bussey, it is necessary that if a fourth line cuts two of the above lines it must intersect the third also. But from the list (2.32) we find that the line through the points 10 of the first line and 8 of the second line passes through the point 1 and does not cut the third line given above. This shows that the geometry cannot be built out of the difference sets by the generating process discussed above.

(4) The points of a finite Euclidean geometry of t dimensions with m points on a line $EG(t, m)$ can be represented by the marks or elements of $GF(m^t)$. A d-flat is represented by the points corresponding to the set of elements $a_0x^{\alpha_0}+a_1x^{\alpha_1}+ \ldots a_dx^{\alpha_d}$ where a's run through the elements of $GF(m)$ subject to the restriction $\Sigma a = 1$. As before the elements corresponding to the points on the above d-flat and the powers of x's reduced (mod m^t-1) and the point corresponding to the element zero replaced by ∞, are represented by

$$E[\Sigma a_i x^{\alpha i},\ \Sigma a = 1, \subset GF(m),\ X \subset GF(m^t)] \quad (2.40)$$

$$\text{and } D[\Sigma a_i x^{\alpha i},\ \Sigma a = 1, \subset GF(m),\ X \subset GF(m^t), \text{ mod } (m^t-1)] \quad (2.41)$$

in general and by $E[\Sigma a_i x^{\alpha i}]$ and $D[\Sigma a_i x^{\alpha i}, \text{ mod } (m^t-1)]$ in particular. As shown in the previous paper, by taking a suitable number of initial flats and carrying on the operation D of (2.41), we get difference sets of certain description. The difference sets with the above properties need not ensure the existence of $EG(t, m)$.

(5) By considering the planes in $EG(3, 2)$ we get the difference set

$$(0, 1, 2, 4), (\infty, 5, 6, 3) \quad (2.50)$$

both of cycle 7 with the property that the differences arising from the former (mod 7) contain all integers less than 7 twice each and in the latter once. We now replace the set (2.50) by

$$(0, 1, 2, 4), (\infty; 1, 2, 4) \quad (2.51)$$

which satisfy the same properties as (2.50) and generate the following planes

$$\left.\begin{array}{ll} 0, 1, 2, 4 & \infty, 1, 2, 4 \\ 1, 2, 3, 5 & \infty, 2, 3, 5 \\ 2, 3, 4, 6 & \infty, 3, 4, 6 \\ 3, 4, 5, 0 & \infty, 4, 5, 0 \\ 4, 5, 6, 1 & \infty, 5, 6, 1 \\ 5, 6, 0, 2 & \infty, 6, 0, 2 \\ 6, 0, 1, 3 & \infty, 0, 1, 3 \end{array}\right\} \quad (2.52)$$

These do not constitute the 14 planes in $EG(3, 2)$ for the planes $(0, 1, 2, 4)$ and $(\infty, 1, 2, 4)$ intersect in 3 points whereas in $EG(3, 2)$ any two planes can intersect in only two points.

(6) It is, however, possible that certain additional requirements beyond the properties of difference sets are needed to establish the existence of a finite geometry. It is hoped to consider these things in detail in a subsequent communication.

§3. Actual Construction of Difference Sets.

In the previous article it has been shown that a difference set can be constructed by a certain operation D from the powers of a primitive element representing points on a d-flat whose equation is given as a linear combination of elements in $GF(m^{t+1})$ or $GF(m^t)$ according as

the geometry is projective or Euclidean. An alternative method of representation of points in $PG(t, m)$ is by ordered sets of elements $(b_0, b_1, \ldots b_t)$ belonging to $GF(m)$ and not all simultaneously zero, two sets $(b_0, b_1, \ldots b_t)$ and $(c_0, c_1, \ldots c_t)$ representing the same point when and only when there exists a non-zero element of $GF(m)$ such that $b_i = \sigma c_i$ $(i = 0, 1, 2, \ldots t)$. In the case of $EG(t, m)$ points are represented by ordered sets of elements $(b_1, b_2, \ldots b_t)$ belonging to $GF(m)$.

The correspondence between the representation of points as elements of $GF(m^r)$ and ordered sets of elements in $GF(m)$ is brought out by the representation of the elements in $GF(m^r)$ as powers of a primitive element or a polynomial of degree less than r in $GF_m[x]$. The polynomial $a_0+a_1x+\ldots+a_{r-1}x^{r-1}$ congruent to a certain element x^β represented as a power of a primitive element supplies the unique correspondence

$$x^\beta \rightarrow (a_0, a_1, \ldots a_{r-1}) \tag{3.10}$$

so that given one the other can be found out.

(2) In this representation a d-dimensional flat in $PG(t, m)$ is represented by $(t-d)$ homogeneous independent set of linear homogeneous equations in $(t+1)$ ordered sets of elements from which all the points on the flat can be deduced as solutions. In the case of $EG(t, m)$, a d-flat is represented by $(t-d)$ consistent and independent set of linear equations in the (t) ordered set of elements in $GF(m)$ and all the points on the flat can be deduced as solutions to these equations. In order to construct a difference set starting from a d-flat in $PG(t, m)$ or $EG(t, m)$ we may take its equation as given above and take the powers of x's corresponding to the solutions of these equations.

(3) In any particular case the simpler of the two representations may be used as a general approach to the problem but much quicker methods are often suggested by the procedure involved in any one of these methods.

(4) It has been shown that by considering a $(t-1)$-flat in $PG(t, m)$ we can find a set of distinct integers

$$d_0, d_1, \ldots d_k^* \tag{3.40}$$

where $k = (m^t-1)/(m-1)$, such that $d_i < v = (m^{t+1}-1)/(m-1)$ for all i and the differences arising from them mod v contain all integers less than v each $\lambda = (m^{t-1}-1)/(m-1)$ times. We may choose the $(t-1)$-flat $c_0+c_1x+\ldots c_{t-1}x^{t-1}$ in which case we get the result that *the d's of* (3.40) *are distinct solutions of*

$$x^{d+iv} = c_0+c_1x+\ldots c_{t-1}x^{t-1} \tag{3.41}$$

for all sets of c's in $GF(m)$ *not simultaneously zero.* As an illustration we may take $t = 3$, $m = 3$; the d's are solutions of

$$x^{d+i40} = c_0+c_1x+c_2x^2 \tag{3.42}$$

where c's are in $GF(3)$ and are not simultaneously zero. With the help of the power cycle table for $GF(3^4)$ we get the solutions as

$$0, 1, 2, 5, 12, 18, 22, 24, 26, 27, 29, 32, 33 \tag{3.43}$$

which constitutes a difference set for $k = 13$, $\lambda = 4$ and $v = 40$.

(5) Taking the representation of a point as an ordered set $(b_0, b_1, \ldots b_t)$ we may take the $(t-1)$-flat defined by $b_r = 0$, in which case *the d's of* (3.40) *are distinct solutions of the correspondences*

$$x^{d+iv} \rightarrow (b_0, b_1, \ldots b_r = 0, \ldots b_t) \tag{3.50}$$

for b's in $GF(m)$ *not simultaneously zero.* In this case we need only go through the table of power cycle for $GF(m^{t+1})$ and take the powers of those elements which are congruent to polynomials with the coefficient of the r-th power zero. Since the power cycle is recorded up to x^v, all distinct solutions of (3.50) can be got from these alone. As an illustration we may choose $t = 3$, $m = 3$ and $b_0 = 0$, i.e. the constant term is zero. Going through the power cycle for 3^4 we find the solution as

$$1, 2, 3, 6, 13, 19, 23, 25, 27, 28, 30, 33, 34 \tag{3.51}$$

This difference set can be derived from (3.43) by the addition of 1 to each of its elements.

(6) We can go a step further and represent the results with reference to certain congruence properties of the minimum function. If

$$x^{t+1}-a_tx^t-\ldots-a_0 \tag{3.60}$$

is a minimum function then all the powers of x can be represented by a polynomial of order less than or equal to t in $GF_m[x]$. If

$$x^\alpha = \xi_\alpha^0+\xi_\alpha^1x+\ldots\xi_\alpha^t\,x^t \tag{3.61}$$

then the ξ's satisfy the recurrence relations

$$\xi^0_{\alpha+1} = a_0\xi^t_\alpha,\ \xi^i_{\alpha+1} = \xi^{i-1}_\alpha + a_i\xi^t_\alpha \quad (i = 1, 2, \ldots t) \tag{3.62}$$

$$\xi^t_{\alpha+1} = a_t\xi^t_\alpha + a_{t-1}\xi^t_{\alpha-1} + \ldots + a_0\xi^t_{\alpha-t} \tag{3.63}$$

with the initial conditions $\xi^i_\alpha = 0$ ($\alpha = 0, 1, \ldots (i-1)$ and v). From this by using the result of the previous para., we get that *the d's of* (3.40) *are distinct solutions of*

$$\xi^r_{d+iv} = 0 \tag{3.64}$$

for any $r = 0, 1, 2, \ldots t$, *where the* ξ^r *satisfy the recurrence relations*

$$\xi^r_{\alpha+1} = a_r\xi^t_\alpha + a_{r-1}\xi^t_{\alpha-1} + \ldots + a_0\xi^t_{\alpha-r} \tag{3.65}$$

deduced from above. It is interesting to see as to how the difference set depends upon the periodicities of functions satisfying linear difference equations.

(7) It has been shown that by considering a $(t-1)$-flat not passing through the point represented by the null element in $GF(m^t)$ we can find a set of $k = m^{t-1}$ integers

$$d_1, d_2, \ldots d_k \tag{3.70}$$

such that $d_i < v = (m^t-1)$ for all i and the differences arising from this (mod v) contain all integers less than v and not divisible by $\theta = (m^t-1)/(m-1)$, $\lambda = m^{t-2}$ times each and those divisible by θ, zero times. We may choose the initial flat $a_0 + a_1x + \ldots + a_{t-1}x^{t-1}$ in which case we get the result that *the d's of* (3.70) *are the solutions of*

$$x^{d+iv} = a_0 + a_1x + \ldots + a_{t-1}x^{t-1} \tag{3.71}$$

where x *is a primitive element of* $GF(m^t)$ *and the a's assume all possible values in* $GF(m)$ *subject to the restriction* $\Sigma a = 1$. For illustration we may take $t = 3$, $m = 3$ in which case the d's are given by

$$D[a_0 + a_1x + a_2x^2;\ \Sigma a = 1 \subset GF(3);\ X \subset GF(27);\ \text{mod } 26] \tag{3.72}$$

With the help of the power cycle table for $GF(3^3)$ we get the d's as

$$0, 1, 2, 8, 11, 18, 20, 22, 23 \tag{3.73}$$

(8) Taking the representation as an ordered set $(b_1, b_2 \ldots b_t)$ we may take the $(t-1)$-flat $b_r = \alpha \neq 0$. Hence we get the result that *the d's of* (3.70) *are the solutions of the correspondences*

$$x^{d+iv} \to (b_1, b_2 \ldots b_r = \alpha, \ldots b_t) \tag{3.80}$$

where α *is a non-zero element of* $GF(m)$ *and others are free in* $GF(m)$. As an illustration we may take $t = 3$, $m = 3$ and take the $(t-1)$-flat, $b_2 = 2$ in which case we have to find the solutions of the correspondences

$$x^{d+i26} \to (b_1, 2, b_3) \tag{3.81}$$

where the b's assume the values 0, 1 and 2. Going through the power cycle for $GF(3^3)$ we find that

$$x^4, x^7, x^{14}, x^{16}, x^{18}, x^{19}, x^{22}, x^{23}, x^{24} \tag{3.82}$$

are congruent to polynomials of the form $b_1 + 2x + b_3x^2$ and hence

$$4, 7, 14, 16, 18, 19, 22, 23, 24 \tag{3.83}$$

gives the required difference set which is obtainable from (3.73) by the addition of 22 to each of its elements.

(9) The difference set obtained from the solutions of

$$x^{d+i26} \to (b_1, 0, b_3) \tag{3.90}$$

is

$$0, 2, 8, 12, 13, 15, 21, 25 \tag{3.91}$$

To this we add ∞, corresponding to the point (0, 0, 0) through which the flat $b_2 = 0$ passes. The distinct set of integers in (3.91) reduced modulo 13 gives the difference set corresponding to the values $t = 2$, $m = 3$ of the theorem in para. (4) of this article. The set (3.91) with ∞ taken as such is of cycle 13, i.e. addition of 13 to all integers does not alter the set.

(10) As before, we can express these results with reference to solutions of linear difference equations. If

$$x^t - a_{t-1}x^{t-1} - \ldots - a_0 \tag{3.10, 0}$$

is a minimum function, then the powers of x's can be represented by polynomials of degree less than or equal to $(t-1)$. If

$$x^\beta = \xi^0_\beta + \xi^1_\beta x + \ldots \xi^{t-1}_\beta x^{t-1} \tag{3.10, 1}$$

then the ξ's satisfy the recurrence relations

$$\xi^0_{\beta+1} = a_0\xi^{t-1}_\beta,\ \xi^i_{\beta+1} = \xi^{i-1}_\beta + a_i\xi^{t-1}_\beta \tag{3.10, 2}$$

$$\xi^{t-1}_{\beta+1} = a_{t-1}\xi^{t-1}_\beta + a_{t-2}\xi^{t-1}_{\beta-1} + \ \ldots\ + a_0\xi^{t-1}_{\beta-t} \tag{3.10, 3}$$

Hence we get the result that *the d's of* (3.70) *are the solutions of*

$$\xi^r_{d+iv} = \alpha \neq 0 \tag{3.10, 4}$$

for any $r = 1, 2, \ldots t$, *where* ξ^r *satisfies the linear difference equation*

$$\xi^r_{\beta+1} = a_r\xi^{t-1}_\beta + \ \ldots\ + a_0\xi^{t-1}_{\beta-r} \tag{3.10, 5}$$

(11) Further aspects of the problem where the a's themselves are determinable from the solutions of certain polynomial equations connecting them will be discussed in a subsequent communication.

(12) In the general case where the number of sets is more than one the following result will be helpful. If

$$a_0x^{\alpha_0} + a_1x^{\alpha_1} + \ \ldots\ a_dx^{\alpha_d} \tag{3.12, 0}$$

is the equation to a d-flat in $PG(t, m)$ or $EG(t, m)$ then

$$\sum_{i=0}^{d} a_ix^{m^r\alpha_i} \tag{3.12, 1}$$

for all integral ($r < t+1$ or t) represents a d-flat belonging to the geometry. *If the differences arising out of* $D[\Sigma a_ix^{\alpha_1}]$ *and* $D[\Sigma a_ix^{m^r\alpha_i}]$ *are not identical then* (3.12, 1) *cannot be obtained from* (3.12, 0) *by multiplication of the latter with any power of* x. The proof is immediate for otherwise the differences will be equal.

(13) This gives a general method of getting at the initial flats which give the difference sets. We start with any d-flat of a known cycle and get the difference set it supplies. The other difference sets are to be obtained by multiplying the integers of the first set by, m, m^2, ... and reduction to appropriate modulus provided the differences arising out of the new sets are not identical with those from any of the previous sets. If the required number of sets are not complete by this process we have to choose another initial flat such that the differences arising out of the difference set it supplies are not identical with those of any set obtained above and obtain another series by multiplying with m, m^2, ... If this does not cover the requisite number some more initial flats have to be chosen such that they cannot be derived from any of the initial flats already used by multiplication with a power of x and fill up the remaining difference sets with their help. This principle will be applied in the following illustrations.

(14) It has been shown in the earlier paper that by considering the lines in $PG(t, m)$ we get the theorem that if $m = p^n$ (p being a prime) and $\theta = (m^{t+1}-1)/(m^2-1)$ is not integral it is possible to find $y = (m^t-1)/(m^2-1)$ sets

$$d_{0j}, d_{1j}, \ \ldots\ d_{mj} \tag{3.14, 1}$$

($j = 1, 2, \ldots y$) such that the differences arising from them mod $v = (m^{t+1}-1)/(m-1)$ contain the integers less than v once and once only. As an illustration we may take $t = 4$, $m = 2$. In any case we can take $a_0 + a_1x$ to be an initial line. The $D[a_0 + a_1x]$ can be obtained from the powers of those elements which are congruent to a first degree polynomial from the table of power cycle corresponding to 2^4. This comes out as (0, 1, 18). The other sets obtained by multiplying this by 2, 2^2, 2^3, 2^4 and reduced to modulus 31 are (0, 2, 5), (0, 4, 10), (0, 8, 20) and (0, 9, 16). The differences arising from these 5 sets are all different from one another and this is the requisite number of sets.

(15) All the difference sets constructed in the previous paper follow from the general principle enunciated here. Thus the difference set

$$(0, 1, 22), (0, 2, 8), (0, 3, 14), (0, 7, 17) \tag{3.15, 1}$$

derived in the earlier paper by considering lines in $EG(3, 3)$, has the property that the differences arising from them mod 26 contain all integers less than 26 and not divisible by 13, once and those divisible by 13, zero times. This can be constructed from the set (0, 1, 22) and two others (0, 3, 14) and (0, 7, 17) obtained by multiplying this with 3 and 3^2 and a fourth set (0, 2, 8) which remains invariant on multiplication by any power of 3.

§ 4. Solutions to Combinatorial Problems.

With the help of the difference sets derived above cyclical solutions to several combinatorial problems can be derived. Some of the important combinatorial problems that have practical applications in the theory of design of experiments in statistics and their solutions derivable from number theory results and finite geometrical configurations are discussed below.

(A) *Kirkman's School Girl Problem.*

(2) The problem originally suggested by T. P. Kirkman is as follows. A school mistress is in the habit of taking her fifteen girls for a daily walk and they are arranged in 5 rows of 3 each so that each girl might have two companions. The problem is to dispose them so that for seven consecutive days no girl will walk with any of her school fellows in any triplet more than once. A generalisation of this is as follows. There are v girls to be formed in n rows of k each to be taken for walk on r consecutive days such that any pair of girls are in company for λ days. The necessary conditions for the solution to exist are

$$vr = bk, \quad \lambda(v-1) = r(k-1), \quad v = nk \qquad (4.20)$$
$$b \geqslant v+r-1$$

The last inequality is due to Bose (1942).

(3) In the earlier paper it has been shown that m^t objects can be arranged in $r = (m^t-1)/(m-1)$ groups such that each group contains all the m^t objects in m sets of m^{t-1} objects each such that any pair of objects are repeated in $\lambda = (m^{t-1}-1)/(m-1)$ sets in the totality. The method of construction is to take a $(t-1)$-flat in $EG(t, m)$ not passing through the point represented by the null element of $GF(m^t)$ and get the difference set

$$d_1, d_2, \ldots d_k \qquad (4.30)$$

associated with it. The arrangement into m sets in the first group is given by

$$d_1+i\theta, d_2+i\theta, \ldots d_k+i\theta \qquad (4.31)$$
$$i = 0, 1, 2, \ldots (m-2)$$

and another set containing the remaining objects, where $\theta = (m^t-1)/(m-1)$. The other groups are obtained from (4.31) by the addition of integers $1, 2, \ldots (\theta-1)$ to each of the above sets and reduction to mod (m^t-1) and filling the last set by the remaining elements. This method of generating the arrangement in the first group can be represented by

$$[(d_1, d_2, \ldots d_k)\, S(\theta)+R] \bmod (m^t-1) \qquad (4.32)$$

and the process of generating the rest of the groups by

$$PC(\theta)\, [(d_1, d_2, \ldots . d_k)\, S(\theta)+R] \bmod (m^t-1) \qquad (4.33)$$

$S(\theta)$ denoting a step θ and $PC(\theta)$ (partial cycle) denoting the groups obtained by the addition of $0, 1, 2, \ldots (\theta-1)$ and R standing for the set of remaining objects of which one object is represented by ∞ which remains invariant when added to any element of the residue classes mod (m^t-1).

This arrangement supplies the solutions to cases where

$$v = m^t, \quad k = m^{t-1}, \quad n = m(= p^s, \text{ prime power}) \qquad (4.34)$$
$$r = (m^t-1)/(m-1), \quad \lambda = (m^{t-1}-1)/(m-1) \qquad (4.35)$$
$$b = [(m^{t+1}-1)/(m-1)]-1 \qquad (4.36)$$

(4) Solutions are always available in the case

$$v = m^t, k = m^d, n = m^{t-d} \qquad (4.40)$$
$$r = \phi(t-1, d-1, m), \lambda = \phi(t-2, d-2, m) \qquad (4.41)$$
$$b = \phi(t, d, m)-\phi(t-1, d-1, m) \qquad (4.42)$$

where

$$\phi(t, d, m) = \frac{(m^{t+1}-1)(m^t-1) \ldots (m^{t-d+1}-1)}{(m^{d+1}-1)(m^d-1) \ldots (m-1)} \qquad (4.43)$$

The method of construction is to take a $(t-1)$-flat in $PG(t, m)$ and list all $(d-1)$-flats lying on it. Through each $(d-1)$-flat there pass m^{t-d}, d-flats which do not lie entirely in the

$(t-1)$-space with which we start. If we omit the points in this $(t-1)$-space, the m^{t-d}, d-flats through a $(d-1)$-flat constitute an arrangement of m^t points of the geometry thus giving one required group. There are as many arrangements as there are $(d-1)$-flats in a $(t-1)$-space. The values of λ and r are derived from the considerations of finite geometrical configurations and are discussed in the earlier paper. This solution can be easily deduced from the consideration of d-flats in $PG(t, m)$ in particular cases and a general solution depending on the difference properties can also be deduced.

(5) We can deduce the solution to Kirkman's original problem by constructing a special transformation of points in $PG(t, 2)$. A point in this geometry can be represented by an ordered set of $(t+1)$ elements belonging to $GF(2)$. If we take the points with the first term zero then there is a correspondence between these points and t elements of $GF(2^t)$. If $a_0+a_1x+a_2x^2+ \ldots +a_{t-1}x^{t-1}-x^t$ is a minimum function for $GF(2^t)$ and x^β and $x^{\beta+1}$ are two elements defined by

$$x^\beta = b_0+b_1x+ \ldots b_{t-1}x^{t-1} \tag{4.50}$$

$$x^{\beta+1} = b_0^1+b_1^1x+ \ldots b_{t-1}^1x^{t-1} \tag{4.51}$$

then

$$\begin{aligned} b_0^1 &= b_{t-1}a_0, \\ b_1^1 &= b_0+b_{t-1}a_1, \\ &\cdots\cdots\cdots\cdots \\ b_{t-1}^1 &= b_{t-2}+b_{t-1}a_{t-1}. \end{aligned} \tag{4.52}$$

This defines a transformation of the ordered sets of points $(b_0, b_1, \ldots b_{t-1})$ the order of transformation being (2^t-1). If we take any point in $PG(t, 2)$ with the first term zero and apply the transformation (4.52) we get (2^t-1) other points, starting with a point for which the first term is 1 and at least one of the other terms is not zero and applying the transformation (4.52) on it we generate (2^t-1) points. The point $(1, 0, 0 \ldots 0)$ transforms into itself. This transformation being linear, transforms d-flats into d-flats and the totality of d-flats generated from a single one is (2^t-1).

(6) In the special case of $PG(3,2)$, there are 35 lines with 3 points on a line. The 15 points in it are represented by 15 non-zero elements

$$x^0, x^1, \ldots x^{14}, \tag{4.60}$$

of $GF(2^4)$. If y is a primitive element in $GF(2^3)$ then the correspondence

$$\begin{gathered} y^0 \to (0, 0, 1),\ y^1 \to (0, 1, 0),\ y^2 \to (1, 0, 0) \\ y^3 \to (1, 0, 1),\ y^4 \to (1, 1, 1),\ y^5 \to (1, 1, 0) \\ y^6 \to (0, 0, 1) \end{gathered} \tag{4.61}$$

defines a transformation of order 7. If we start with the point $(0, 0, 0, 1)$ in $PG(3, 2)$ and apply (4.61) on the last three coordinates we get the points

$$(0, 0, 0, 1),\ (0, 0, 1, 0),\ (0, 1, 0, 0),\ (0, 1, 0, 1),\ (0, 1, 1, 1),\ (0, 0, 1, 1),\ (0, 1, 1, 0) \tag{4.62}$$

which can be identified as

$$x^0, x^1, x^2, x^9, x^7, x^{12}, x^{13} \tag{4.63}$$

Thus the transformation given above transforms the points (recording only the powers) cyclically.

$$0 \to 1 \to 2 \to 9 \to 7 \to 12 \to 13 \to 0 \tag{4.64}$$

Similarly starting with the point $(1, 0, 0, 1)$ we get the cycle

$$4 \to 10 \to 14 \to 11 \to 6 \to 5 \to 8 \to 4 \tag{4.65}$$

The point 3 goes into itself. Starting with an initial set of lines which contains all the points of the geometry and applying (4.64) and (4.65) we get the required arrangement, this method being applicable in the general case of lines in $PG(t, 2)$. Starting with the arrangement on the first day, we derive all the others.

1st day	(0, 5, 10),	(1, 6, 11),	(2, 7, 12),	(3, 8, 13),	(4, 9, 14)
2nd ,,	(1, 8, 14),	(2, 5, 6),	(9, 12, 13),	(3, 4, 0),	(10, 7, 11)
3rd ,,	(2, 4, 11),	(9, 8, 5),	(7, 13, 0),	(3, 10, 1),	(14, 12, 6)
4th ,,	(9, 10, 6),	(7, 4, 8),	(12, 0, 1),	(3, 14, 2),	(11, 13, 5)
5th ,,	(7, 14, 5),	(12, 10, 4),	(13, 1, 2),	(3, 11, 9),	(6, 0, 8)
6th ,,	(12, 11, 8),	(13, 14, 10),	(0, 2, 9),	(3, 6, 7),	(5, 1, 4)
7th ,,	(13, 6, 4),	(0, 11, 14),	(1, 9, 7),	(3, 5, 12),	(8, 2, 10)

(B) *Incomplete Balanced Designs.*

(7) An arrangement with v objects in b sets of $k<v$ each is said to be an incomplete balanced design if each object is used r times and every pair of objects occurs in λ sets. When the b sets form into r groups of n sets each such that each group contains all the v objects, the incomplete balanced design is said to be resolvable. Some of them have been already considered in the above paras. We identify the v objects with the points of a finite geometry and the b sets with all the d-flats in it. Then as observed by Bose (1939) we get solutions to incomplete balanced designs of certain type. Since the finite geometries $PG(t, m)$ and $EG(t, m)$ are capable of compact representation by the use of difference sets, the solutions to these designs can be compactly represented by the same sets. We give below two tables giving the non-resolvable and resolvable designs. Some of the designs which are not derivable by these methods have also been included with due references. The methods of derivation have also been indicated to make the tables self-explanatory. Only those designs which are useful in practical experimentation have been recorded. Other designs with values higher than those given here can be obtained in the manner discussed in the article and some other special devices.

TABLE 2.

Non-resolvable balanced designs.

Serial No.	v	b	r	k	λ	Solution.
1	6	10	5	3	2	(1, 2, 3), (1, 3, ∞) mod 5.
2	7	7	3	3	1	(1, 2, 4) mod 7.
3	9	18	8	4	3	(1, 2, 3, 5), (1, 4, 5, 8) mod 9.
4	10	15	6	4	2	B.S from (20).
5	10	30	9	3	2	(1, 2, 3), (1, 3, 7), (1, 5, ∞) mod 9 and PC (1, 4, 7) mod 9.
6	11	11	5	5	2	(1, 3, 4, 5, 9) mod 11.
7	13	13	4	4	1	(1, 2, 4, 10) mod 13.
8	13	26	6	3	1	(1, 3, 9) (2, 6, 5) mod 13.
9	15	15	7	7	3	(1, 2, 3, 8, 10, 13, 14) mod 15.
10	19	57	9	3	1	(1, 7, 11), (2, 3, 14), (4, 6, 9) mod 19.
11	19	19	9	9	4	(1, 4, 5, 6, 7, 9, 11, 16, 17) mod 19.
12	21	21	5	5	1	(1, 4, 5, 10, 12) mod 21.
13	28	36	9	7	2	B.S from (15).
14	31	31	6	6	1	(1, 2, 4, 11, 15, 27) mod 31.
15	37	37	9	9	2	(1, 7, 9, 10, 12, 26, 33, 34, 16) mod 37.
16	41	82	10	5	1	(1, 10, 16, 18, 37), (5, 8, 9, 21, 39) mod 41.
17	57	57	8	8	1	(1, 4, 6, 14, 15, 21, 33, 37) mod 57.
18	73	73	9	9	1	(1, 2, 4, 8, 16, 32, 37, 55, 64) mod 73.
19	91	91	10	10	1	(1, 2, 7, 11, 24, 27, 35, 42, 54, 56) mod 91.
20	16	16	6	6	2	$(a_1, a_2, a_3, b_1, c_4, d_1)$ dicyclic.
21	25	50	8	4	1	(a_1, a_2, b_1, e_5) (a_1, a_3, c_1, d_4) dicyclic.
22	31	31	10	10	3	$(a_1, a_2, a_4, b_1, b_2, b_4, c_1, c_2, c_4, d_6)$ $(a_1, a_6, b_2, b_5, c_3, c_4, d_3, d_5, d_6, e)$ $(a_2, a_5, b_3, b_4, c_1, c_6, d_3, d_5, d_6, f)$ $(a_3, a_4, b_1, b_6, c_2, c_5, d_3, d_5, d_6, g)$ } mod 7 (for the suffixes keeping a, b, . . . fixed). and $(a_1, a_2, a_3, a_4, a_5, a_6, a_7, e, f, g)$ $(b_1, b_2, b_3, b_4, b_5, b_6, b_7, e, f, g)$ $(c_1, c_2, c_3, c_4, c_5, c_6, c_7, e, f, g)$
23	21	30	10	7	3	B.S from (22)

(22) is due to Bhattacharya (1945).

(1) to (21) are derivable from the considerations of this paper but many solutions have been already given in Fisher and Yates' tables (1943).

Use of table (2).

$(x, y, z \ldots)$ mod n means that all the blocks can be generated from this by adding 1, 2, . . . and replacing any integer which exceeds n by the integer congruent to mod n. $PC(\theta)$ means that the above process should be carried on till only θ blocks are obtained, the $(\theta+1)$-th block being identical with the first.

$B.S$ from (X) means that the design can be obtained by cutting out one block and all the objects in it from the design corresponding to X.

(20) and (21). These solutions are called dicyclic solutions and are taken from Fisher and Yates' tables. The process of development is to fix $a, b, c, \ldots$ first and change the suffixes cyclically and then change $a, b, c, \ldots$ cyclically. Besides these there are a few designs which may be recorded here for completeness.

Solution for $v = 25 = b$, $r = 9 = k$, $\lambda = 3$.

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

The design for $v = 16$, $b = 24$, $r = 9$, $k = 6$, and $\lambda = 3$ is obtained by omitting the integers 17 to 25 from the above. The solution given above is due to Bhattacharya (1944). The solution for $v = 28$, $b = 63$, $r = 9$, $k = 4$ and $\lambda = 1$ does not possess an elegant representation.

TABLE 3.

Resolvable balanced designs.

Serial No.	v	b	r	k	λ	n	Solution.
1	8	14	7	4	3	2	PC (7) $[(1, 2, 3, 5)+R]$ mod 7.
2	9	12	4	3	1	3	PC (4) $[(1, 6, 7)\ S(4)+R]$ mod 8.
3	16	20	5	4	1	4	PC (5) $[(1, 3, 4, 12)\ S(5)+R]$ mod 15.
4	25	30	6	5	1	5	PC (6) $[(1, 3, 16, 17, 20)\ S(6)+R]$ mod 24.
5	49	56	8	7	1	7	PC (8) $[(1, 2, 5, 11, 31, 36, 38)\ S(8)+R]$ mod 48.
6	64	72	9	8	1	8	PC (9) $[(1, 6, 8, 14, 38, 48, 49, 52)\ S(9)+R]$ mod 63.
7	81	90	10	9	1	9	PC (10) $[(1, 13, 35, 48, 49, 66, 72, 74, 77)\ S(10)+R]$ mod 80.
8	15	35	7	3	1	5	$[(1, 6, 11)\ S(1)]$. CT (1 . 2 . 3 . 10 . 8 . 13 . 14) (5 . 11 . 15 . 12 . 7 . 6 . 9).
9	21	70	10	3	1	7	$[(1, 4, 10), (2, 5, 11), (3, 6, 12), (7, 14, 18), (8, 15, 16), (9, 13, 17), (19, 20, 21)]$. CT (1 . 4 . 7 . 10 . 13 . 16 . 19) (2 . 5 . 8 . 11 . 14 . 17 . 20) (3 . 6 . 9 . 12 . 15 . 18 . 21). $[(1, 6, 11)\ CT], [(2, 4, 12)\ CT], [(3, 5, 10)\ CT]$.

(1) to (8) follow from the consideration of this paper. Use has been made of Desargusian difference sets given by Bose (1942*a*).

(9) has been copied from page 280 in Ball's Mathematical recreations.

Use of table (3).

The method of generating the complete solution will be indicated with reference to a particular solution No. (3) of the table.

[(1, 3, 4, 12) $S(5)+R$] stands for $n = 4$ sets of $k = 4$ each containing all the $v = 16$ objects. The method of generation is to take the initial set (1, 3, 4, 12) and get $(n-2) = 2$ (for this problem) more sets by the addition of 5 and 10. (In general if $S(\theta)$ is found then $(n-2)$ more sets are generated by the addition $\theta, 2\theta, \ldots (n-2)\theta$ and reduction to reminder after dividing by $(v-1)$ indicated in the table as mod $(v-1)$.) In this case $(v-1) = 15$. Hence we get the $(n-1)$ sets including the initial set as (1, 3, 4, 12), (6, 8, 9, 2), (11, 13, 14, 7). To this we add the remaining set of elements in 15 and a 16th element to be denoted by ∞ (R stands for remaining elements in $(v-1)$ and a v-th element to be denoted by ∞). Thus we get the 4 sets of the first group as

$$[(1, 3, 4, 12)\ S(5)+R] = (1, 3, 4, 12), (6, 8, 9, 2), (11, 13, 14, 7), (5, 10, 15, \infty)$$

The other $4=(r-1)$ groups are obtained by operating $PC(5)$ on this, i.e. by adding 1, 2, 3, 4 to each of the above sets, the element ∞ remaining unaffected. Thus the 2nd, 3rd, 4th and 5th sets are

(2, 4, 5, 13)	(7, 9, 10, 3)	(12, 14, 15, 8)	(6, 11, 1, ∞)
(3, 5, 6, 14)	(8, 10, 11, 4)	(13, 15, 1, 9)	(7, 12, 2, ∞)
(4, 6, 7, 15)	(9, 11, 12, 5)	(14, 1, 2, 10)	(8, 13, 3, ∞)
(5, 7, 8, 1)	(10, 12, 13, 6)	(15, 2, 3, 11)	(9, 14, 4, ∞)

Addition of 5 brings the last set back to the first set. $PC(\theta)$ (partial cycle) stands for generation of other sets by the addition $1, 2, \ldots (\theta-1)$.

(8) and (9) require special mention. The contents of rectangular brackets always give a set. The rest of the sets are generated by a cyclical transformation indicated below; (1 . 2 . 3 . 10 . 8 . 13 . 14) means changing 1 to 2, 2 to 3, ... and 14 to 1. For further particulars reference may be made to para. 6 of this section.

(C) *Hypercubes of Strength d.*

(8) Let us consider t factors $A_1, A_2, \ldots A_t$ each of which assumes m different values called the levels of a factor. The m levels of the i-th factor may be represented by $1_i, 2_i, \ldots m_i$. We define an ordered set $(x_1 y_2 z_3 \ldots u_t)$ as a combination of t factors where $x, y, z \ldots u$ can assume values from 1 to m. There are m^t combinations on the total of which a subset of m^k combinations may be called a (t, m, k) *array*. A (t, m, k) array is said to be of *strength* d if all the m^d combinations of any d factors out of t occur an equal number (m^{k-d}) of times, in which case the array may be represented by (t, m, k, d). Evidently $t \geqslant k \geqslant d$. The general problem is the construction of (t, m, k, d) arrays and discuss the optimum values of t and d for given values of m, k, d and m, k, t respectively.

(9) The array $(t, m, 2, 2)$ may be identified with the existence of $(t-2)$ orthogonal latin squares of side m. This may be taken as an alternative definition of mutually orthogonal latin squares which has led to the above generalisation to orthogonal cubes and hypercubes of a more useful type different from those defined by Kishen (1942). His consideration of first order cubes leads to arrangements of strength 2 only. The above definition leads to the possibilities of k dimensional hypercubes of strength $d \leqslant k$.

(10) The existence of the array (t, m, k, d) leads to confounded factorial arrangements consisting of t factors each at m levels arranged in blocks of m^k plots, preserving all main effects and interactions up to the order $(d-1)$. Its use in getting balanced arrangements for asymmetrical factorial designs has been discussed by the author in (Rao: 1943).

(11) It is shown below that the array (t, m, k, d) can always be constructed for optimum values of t and d to be determined when m is a prime or a prime power with the help of k dimensional projective geometry with $(m+1)$ points on a line.

(12) We take a $(k-1)$-flat in $PG(k, m)$ and call it the flat at infinity. Through each $(k-2)$-flat on the $(k-1)$-flat at infinity there pass m, $(k-1)$-flats (excluding the one at infinity) which do not meet in any finite point (all points other than those on the $(k-1)$-flat at infinity are called finite points) in which case they are said to be parallel. If we identify the $(k-2)$-flats at infinity with factors and the m parallel $(k-1)$-flats through each of them with the m levels

of that factor by some method of identification, then any of the m^k finite points in $PG(k, m)$ can be uniquely represented by an ordered set depending on the nature of the flats passing through them. We thus get m^k combinations corresponding to m^k finite points. Since any two $(k-1)$-flats belonging to different $(k-2)$-flats at infinity as vertices intersect in a $(k-2)$-flat we get the result that any combination of any two factors occur in m^{k-2} combinations corresponding to m^{k-2} finite points on this $(k-2)$ flat.

Hence we get the result that the optimum value of t for $(t, m, k, 2)$ is the number of $(k-2)$-flats lying on a $(k-1)$-flat. This number is $(m^k-1)/(m-1)$. This leads to an important result in the theory of factorial experimentation in the design of experiments. *The maximum number of factors each at m levels that can be used in an experiment with blocks of size m^k (plots) such that all the main effects and first order interactions are preserved is given by $(m^k-1)/(m-1)$.*

(13) The conditions for the array $(t, m, k, 3)$ are satisfied if any three $(k-1)$-flats through 3 different vertices or $(k-2)$-flats at infinity meet in a $(k-3)$-flat. This requires that the $(k-2)$-flats at infinity which are to be identified with factors must be such that none of them passes through the intersection of any other two, i.e. no three of the chosen $(k-2)$-flats infinity should have a common $(k-3)$-flat at infinity. The optimum value of t is the number of $(k-2)$-flats at infinity which possess this property. We may determine this number for $m = 5$, $k = 3$. We need consider a plane [$(k-1)$-flat] with 5^2+5+1 points and lines. These lines are to be identified with factors. In order to satisfy the above conditions we have to choose a set of lines such that no three of them have a common point. This may be detected by actually finding the lines and selecting properly. In this case we get the number of such lines as 4, 6 and 6 for the values of $k = 3$ and $m = 3$, 4 and 5 respectively. For the actual construction of the array we have to consider the geometry of k dimensions.

(14) From this it follows that if we are using blocks of 5^3 plots the maximum number of factors, each at 5 levels, that can be allowed in order to preserve main effects and interactions up to the second order is 6. In the case of $m = 3$ and 4, the corresponding values are 4 and 6 respectively.

(15) In general the highest value of t for which (t, m, k, d) can be constructed is the number of $(k-2)$-flats at infinity such that no d of them should have a common flat at infinity of dimensions less than or equal to $(k-d)$. The method of constructing is to take the $(k-2)$-flats satisfying the above condition as vertices to be identified with the factors and get ordered sets for the m^k finite points corresponding to the $(k-1)$-flats passing through them from the chosen vertices as indicated in para. (11) of this section.

(16) The general methods of finding this optimum value and the construction of arrays of strength d and their application in the problem of confounding in symmetrical and asymmetrical factorial experiments will be considered in detail in a subsequent communication. It appears that these arrays supply proper representation of orthogonal cubes and hypercubes without resorting to diagrammatic representation.

References.

Bhattacharya, K. N. (1944). On a new symmetrical incomplete block design. *Bull. Cal. Math. Soc.*, **36**, 91–96.

——— (1945). The balanced incomplete block design $v = b = 31$, $r = k = 10$, $\lambda = 3$. *Proc. Ind. Sc. Cong. 32nd I.S.C.*, p. 166.

Bose, R. C. (1942*a*). The affine analogue of Singer's theorem. *Journ. Ind. Math. Soc.*, **6**, 1–15.

——— (1942*b*). A note on the resolvability of balanced incomplete block designs. *Sānkhya*, **6**, pt. 2, 105–110.

——— (1939). On the construction of balanced incomplete block designs. *Ann. of Eugen.*, **9**, 353–399.

Bose, R. C., Chowla, S., and Rao, C. R. (1944). On the integral order (mod p) of quadratics x^2+ax+b, with applications to the construction of minimum functions for $GF(p^2)$, and to some number theory results. *Bull. Cal. Math. Soc.*, **36**, 153–174.

Kishen, K. (1942). On latin and hypergraeco latin cubes and hypercubes. *Current Science*, **11**, 98-99.

Rao, C. R. (1945). Finite geometries and certain derived results in number theory. *Proc. Nat. Inst. Sc. India*, **11**, 136–149.

Rao, C. R. (1943). Thesis submitted to the Calcutta University.