ON THE CONSTRUCTION OF BOSE CHAUDHURI MATRICES WITH THE HELP OF ABELIAN GROUP CHARACTERS

by

DOMINIQUE C. FOATA

Institute of Statistics
Mimeograph Series No. 278
March, 1961

UNIVERSITY OF NORTH CAROLINA
Department of Statistics
Chapel Hill, N. C.

Mathematical Sciences Directorate
Air Force Office of Scientific Research
Washington 25, D. C.

AFOSR Report No. 489

ON THE CONSTRUCTION OF BOSE-CHAUDHURI MATRICES WITH THE HELP OF ABELIAN GROUP CHARACTERS

by

Dominique C. Foata
University of North Carolina

March, 1961

Contract AF 49(638)-213

It is shown how matrices used in error-correcting codes can be derived from Abelian group characters.

Institute of Statistics
Mimeograph Series No. 278

ON THE CONSTRUCTION OF BOSE-CHAUDHURI MATRICES WITH THE HELP OF ABELIAN GROUP CHARACTERS *

by

Dominique C. Foata
University of North Carolina

Bose [3] has shown that the existence of an $n \times r$ matrix A with entries from GF(s) (s prime power) having the P_d property that any d rows of A are independent, was equivalent to the existence of an (n, n-p) s-ary t-error correcting and (t + 1)-error-detecting group code if d = 2t + 1. He also proved that for d = 2t, it was equivalent to the existence of a $\frac{1}{s^{n-p}} \cdot s^n$ fractionally replicated factorial design in which no t-factor or lower order interaction was aliased with any t-factor or lower order interaction.

Thus we can build error-correcting codes or fractionally replicated factorial designs as soon as we have constructed such matrices having the P_d-property. Bose and Ray-Chaudhuri [1] and [2] have given an explicit method of construction in the binary case. Peterson [4] has investigated some properties of the codes built from these matrices. In particular he gave the exact value of the ranks of these matrices. Finally Zierler [6] has generalized these results to the s-ary case (s prime power).

In this paper using the theory of group characters we reformulate these results and show how these matrices can be obtained from the

---

*This research was supported in part by the United States Air Force Office of Scientific Research of the Air Research and Development Command, under Contract No. AF(638)-213. Reproduction in whole or in part is permitted for any purpose of the United States Government.

character tables of cyclic groups. Hence considering character tables of Abelian groups we can obtain an analogous construction and so a new family of matrices having the P_d-property.

1.

In this section we define the P_d-property over characters of an Abelian group and investigate some properties involved by this definition.

Let G be an Abelian group of order g whose invariants are:

$h_1, h_2, \ldots, h_r$

We know that these invariants are characterized by the following properties:

(i) G is a direct sum of r cyclic groups $G_1, G_2, \ldots, G_r$ of orders $h_1, h_2, \ldots, h_r$ respectively

(ii) $h_{i+1} / h_i \quad (i = 1,2,\ldots,(r-1))$

Thus every element a of G may be uniquely represented in the form:

$a = c_1^{a_1} c_2^{2_2} \ldots c_r^{a_r}$ or simply $(a_1 a_2 \ldots a_r)$

with $(0 \leq a_1 \leq h_1-1;\ 0 \leq a_2 \leq h_2-1;\ \ldots; 0 \leq a_r \leq h_r -1)$

Later on we shall speak about the r "coordinates" of a.

Furthermore if Ω is a field whose characteristic does not divide $h=h_1$ and if ζ_i is an h_i th primitive root of unity in Ω $(i=1,2,\ldots,r)$, the characters of the group G are given by:

$$\chi)u_1,u_2,\ldots,u_r) : a = (a_1 a_2,\ldots,a_r) \longrightarrow \zeta_1^{u_1 a_1} \zeta_2^{u_2 a_2} \ldots \zeta_r^{u_r a_r}$$

$(0 \leq u_1 \leq h_1-1,\ldots,0 \leq u_r \leq h_r-1) \quad a \in G$

(See Van der Waerden page 175 vol. 2)

We will also denote the character $\chi(u_1,u_2,\ldots,u_r)$ by $\zeta_1^{u_1}\zeta_2^{u_2}\ldots\zeta_r^{u_r}$.

As h_i divides h for all $i=2, \ldots, r$, we can take ζ_i as a well-defined power of $\zeta_1=\zeta$ and thus all the images of the elements of G under all the characters will be powers of ζ.

In writing down the character table of G, let us make each row correspond to one element of the group G and each column to one character, in a 1-1 manner. At the intersection of the row a ($a \in G$) and the column χ (χ a character of G) we write the image of a under χ, i.e. $\chi(a)$. Hence the above statement simply says that all the entries of the character table of G are powers of ζ.

Now let p be a prime number not dividing h and let p have the order m in the residue system modulo h ($p^m \equiv 1$ (h) and $p^{m'} \not\equiv 1$ (h) for $m' < m$). Furthermore let $c = \frac{p^m-1}{h}$ and n be a primitive root of the Galois field $GF(p^m)$. Then n^c is an $h^{\underline{th}}$ primitive root of unity in $GF(p^m)$. Hence if we take $GF(p^m)$ for the field Ω and x^c for ζ, all the entries of the character table of G will be elements of the Galois field $GF(p^m)$ and all the properties on the group characters will be preserved. In particular, as the character table of an Abelian group of order g is a non-singular matrix of order g, we have:

Proposition (1.1) Given an Abelian group G of order g whose invariants are $(h, h_2, \ldots, h_r)$ and a prime p not dividing h, we can construct a non-singular matrix of order g whose entries are from $GF(p^m)$, m being the order of p in the residue system modulo h.

In the following it is assumed that the prime p has been definitely chosen (prime to the order g of the group) and the characters take their values in the well-defined field $GF(p^m)$, m being fixed by the choice of p. Moreover the character table or the group of the characters of G will be designated by $\Sigma(G,p,m)$ or simply Σ.

Let us recall the definition of the P_d property introduced by R. C. Bose [1]:

<u>Definition</u> 1. A matrix whose entries are from a field Ω, has the P_d property if any d rows of this matrix are linearly independent

We shall also say:

<u>Definition</u> 2. A set of e characters $(\chi_1 \chi_2 \ldots \chi_e)$ of the group Σ (G, p, m) has the P_d property (over $GF(p^m)$) if the submatrix of the character table Σ, formed by the e columns $\chi_1, \chi_2, \ldots, \chi_e$ is such that any d rows are linearly independent.

Before introducing the definition of the P_d property over a subfield, let us define an equivalence relation among the characters:

It is known that to each divisor n of m corresponds a subfield $GF(p^n)$ of $GF(p^m)$; and the Galois group of $GF(p^m)$ over $GF(p^n)$ is the cyclic group Φ of order $m_1 = \frac{m}{n}$ generated by:

$$\alpha \longrightarrow \alpha^q \qquad q = p^n$$
$$\alpha \in GF(p^m)$$

Hence the definition:

<u>Definition</u> 3. Two characters χ_1 and χ_2 of Σ (G,p,m) are equivalent modulo Φ (n) if there exists an integer e such that:

$$\chi_1 = \chi_2^{q^e} \qquad (q = p^n)$$

As Φ is cyclic and $\chi^{p^m} = \chi^{q^{m_1}} = \chi$ for all χ, this relation is evidently an equivalence relation.

We denote the equivalence classes modulo Φ (n) by $\chi_1^*, \chi_2^*, \ldots$ and the set of characters in the class χ^* containing the character χ by $\{\chi^*\}$.

Definition 4. (P_d property over a subfield)

A set of e characters $(\chi_1\chi_2\ldots\chi_e)$ of Σ (G,p,m) has the P_d property over $GF(p^n)$ (n divisor of m) if any d row vectors of the submatrix $(\chi_1\chi_2\ldots\chi_e)$ of Σ are linearly independent over $GF(p^n)$, i.e. if $v_{i_1}, v_{i_2}, \ldots, v_{i_d}$ are d row vectors of the submatrix $(\chi_1\ \chi_2\ \ldots\chi_e)$, a relation of the form,

$$\lambda_1 v_{i_1} + \lambda_2 v_{i_2} + \ldots + \lambda_d v_{i_d} = 0 \text{ cannot hold}$$

for $\lambda_1, \lambda_2, \ldots, \lambda_d \in$ subfield $GF(p^n)$.

We show:

Proposition(1.2) If $(\chi_1,\chi_2,\ldots,\chi_e)$ of $\Sigma(G,p,m)$ has the P_d property over $GF(p^m)$, then $(\chi_1^*\ \chi_2^*\ \ldots\chi_e^*)$ has the P_d property over $GF(p^n)$.

It is sufficient to show that if

$$\lambda_1\ \chi(a_k) + \lambda_2\ \chi(a_2) + \ldots + \lambda_d\ \chi(a_d) = 0$$

$$\lambda_1\ \lambda_2\ \ldots\ \lambda_d \in GF(p^n)$$

$$a_1, a_2, \ldots, a_d \in G$$

$$\chi \in \Sigma_1\ (G,p,m)$$

then the same linear relation holds if we replace χ by any other character of the equivalence class to which χ belongs.

Indeed as $\alpha \longrightarrow \alpha^{p^n}$ is an antomorphism of $GF(p^m)$ leaving the elements of $GF(p^n)$ invariant elementwise, we have:

$$0 = \Big(\sum_{i=1}^{d} \lambda_i\ \chi(a_i)\Big)^q = \sum_{\substack{i=1\\(q=p^n)}}^{d} \lambda_i^q\ \chi^q(a_i) = \sum_{i=1}^{d} \lambda_i\ \chi^q(a_i)$$

Thus the same relation holds for χ^q and hence for $\chi^{q^2}, \chi^{q^3}, \ldots, \chi^{q^{(m_1-1)}}$, that is, for all the characters of the class χ^* containing χ.

Conversely:

Proposition (1.3) If the set of classes $(\chi_1^*, \chi_2^*, \ldots, \chi_e^*)$ has the P_d property over $GF(p^n)$, then $(\{\chi_1^*\}, \{\chi_2^*\}, \ldots, \{\chi_e^*\})$ has the P_d-property $GF(p^m)$.

Suppose there exist d elements of G, $a_1, a_2, \ldots, a_d$ such that

$$\sum_{i=1}^{d} \lambda_i \chi(a_i) = 0 \qquad \lambda_i \in GF(p^m) \qquad (i=1,\ldots,d)$$

and this relation holds for all the characters χ from $(\{\chi_1^*\}, \{\chi_2^*\}, \ldots, \{\chi_e^*\})$.

Then as $\alpha \rightarrow \alpha^q$ $(q=p^n)$ is an automorphism of $GF(p^m)$,

$$\sum_{i=1}^{d} \lambda_i \chi(a_i) = 0 \Longrightarrow \sum_{i=1}^{d} \lambda_i^q \chi^q(a_i) = \sum_{i=1}^{d} \lambda_i^{q^2} \chi^{q^2}(a_i) = \ldots = \sum_{i=1}^{d} \lambda_i^{q^{(m_1-1)}} \chi^{q^{(m_1-1)}}(a_i) = 0$$

Hence:

$$\sum_{i=1}^{d} (\lambda_i + \lambda_i^q + \ldots + \lambda_i^{q^{(m_1-1)}}) \chi(a_i) = 0$$

since the above relation is assumed to hold for all the characters of of the same equivalence class.

But on the other hand $\mu_i = (\lambda_i + \lambda_i^q + \ldots + \lambda_i^{q^{(m_1-1)}})$ is an element of $GF(p^n)$ since $\mu_i^q = \mu_i$ $(i=1\ldots d)$.

Hence we have found a linear relation over $GF(p^n)$ between d elements of G:

$$\sum_{i=1}^{d} \mu_i \chi(a_i) = 0 \qquad \mu_i \in GF(p^n), \quad i=1,\ldots,d \quad \text{which}$$

holds for all the elements of $(\{\chi_1^*\}, \ldots, \{\chi_e^*\})$ i.e., for the classes $(\chi_1^*, \ldots, \chi_e^*)$ themselves and this contradicts our hypothesis.

If it happened that $\lambda_i + \lambda_i^q + \ldots + \lambda_i^{q^{(m_1-1)}}$ were null for all $i=1,\ldots,d$, we would multiply the equality $\sum_{i=1}^{d} \lambda_i \chi(a_i) = 0$ by a suitable element ν of $GF(p^m)$ such that the relation:

$$\nu \lambda_i + (\nu \lambda_i)^q + \dots + (\nu \lambda_i)^{q^{m_1-1}} = 0$$

would not hold for all the λ_i's. This is always possible since the equation:

$\lambda + \lambda^q + \dots + \lambda^{q^{m_1-1}} = 0$ is not satisfied by all the (q^m-1) non null elements of $GF(p^m)$.

Thus we can say:

Proposition 1.4. The set $(\chi_1^*, \chi_2^*, \dots, \chi_e^*)$ of e distinct classes modulo Φ (n) of Σ (G,p,m) has the P_d property over $GF(p^n)$, if and only if, the set $(\{\chi_1^*\}, \{\chi_2^*\}, \dots, \{\chi_e^*\})$ has the P_d property over $GF(p^m)$.

In particular, if we take all the classes modulo $\Phi(n)$, we exhaust all the characters of the group; and since the character table is non-singular or has the P_g property over $GF(p^m)$, we have:

Proposition 1.5. The set of all the classes modulo $\Phi(n)$ has the P_g property over $GF(p^n)$.

As $\chi^h = 1$ for all $\chi \in \Sigma$ (G,p,m), the inverse of χ is given by:

$$\bar{\chi} = \chi^{h-1}$$

Hence, if $\chi_1 \equiv \chi_2$ modulo $\Phi(n)$

i.e. $\chi_1 = \chi_2^{q^k}$ taking the (h-1) st power of each member, we obtain:

$$\chi_1^{(h-1)} = (\chi_2^{h-1})^{q^k} \quad \text{or } \bar{\chi}_1 = \bar{\chi}_2^{q^k}$$

or $\bar{\chi}_1 \equiv \bar{\chi}_2$ modulo $\Phi(n)$.

Thus we can speak of the inverse of a class χ^*, we shall denot by $\bar{\chi}^*$.

Proposition 1.6. If $(\chi_1^*, \chi_2^*, \dots, \chi_e^*)$ has the P_d property over $GF(p^n)$, then $(\bar{\chi}_1^*, \bar{\chi}_2^*, \dots, \bar{\chi}_e^*)$ has the P_d property over $GF(p^n)$.

For, if $\sum_{i=1}^{d} \lambda_i \chi(ai) = 0 \qquad \lambda_i \in GF(p^n)$,

then $\sum_{i=1}^{d} \lambda_i \bar{\chi}(a_i^{-1}) = 0$, since $\chi(a^{-1}) = \bar{\chi}(a)$

Hence each linear relation between d row vectors of the submatrix $(\chi_1,\chi_2,\dots,\chi_e)$ where $\chi_1 \in \chi_1^*,\dots,\chi_e \in \chi_e^*$ implies a linear relation between d row vectors of the submatrix $(\bar\chi_1,\bar\chi_2,\dots,\bar\chi_e)$, where $\bar\chi_1 \in \bar\chi_1^*, \dots, \bar\chi_e \in \bar\chi_e^*$

Notation: We designate by n_i^* the number of distinct characters contained in the class χ_i^*.

Definition 4: n being gixed as divisor of m, we say that a character χ of $\Sigma(G,p,m)$ belongs to the Galois field $GF(p^e)$ if e is the least multiple of n such that $GF(p^e)$ contains all the images $\chi(a)$ $(a\epsilon G)$.

Proposition 1.7. If χ belongs to $GF(p^e)$, the number n^* of characters of the class χ^* is equal to: $n^* = e_1 = \frac{n}{e}$

For if χ belongs to $GF(p^e)$, all the characters contained in χ^* also belong to $GF(p^e)$.

Thus $[\chi(a)]^{p^e} = [\chi(a)]^{q^{e_1}} = \chi(a)$ and the sequence

$\chi(a),\chi(a)^q,\dots,\chi(a)^{q^{m_1-1}}$ can only have e_1 distinct elements.

Hence the class χ^* only contains $n^* = e_1$ distinct characters.

Finally we remark:

Proposition 1.8. If a set of characters of $\Sigma(G,m,p)$, $(\chi_1,\chi_2,\dots,\chi_e)$ has the P_d property, then the set $(\chi\chi_1,\chi\chi_2,\dots,\chi\chi_e)$ has the P_d property.

(We denote by $\chi\chi_i$ the character: $a \longrightarrow \chi(a)\ \chi_i(a)$)

For if there is a relation: $\sum_{i=1}^{d} \lambda_i\ \chi(a_i)\ \chi_j(a_i) = 0$

for $j = 1 \dots e$, where $\lambda_i \in GF(p^m)$ $i = 1\dots d$.

Then, $\lambda_i\ \chi(a_i) = \mu_i$ is an element of $GF(p^m)$.

Hence there exists a relation:

$$\sum_{i=1}^{d} \mu_i\ \chi_j(ai)=0 \quad j = 1 \dots e$$

which contradicts the hypothesis of the P_d property.

<u>Example 1</u>: Consider the cyclic group G_{15} of order $g = 15$.

Choose $p = 2$, $(2, 15) = 1$, and 2 has the order 4 in the residue system modulo 15

$$2^4 \equiv 1\ (15)$$

Hence x being a primitive root of $GF(2^4)$, in fact a 15^{th} root of unity in this field, we can take our field Ω, into which the characters take their values, as the Galois field $GF(2^4)$.

The characters of $\Sigma(G_{15}, 2, 4)$ are so:

$$\begin{array}{ccc} \zeta^u & : & c^a \longrightarrow x^{ua} \\ u = 0,1,\ldots,14 & & a=0,1,\ldots,14 \end{array}$$

To $n = 1$ corresponds the equivalence relation $\Phi(1)$ and the following equivalence classes:

$$\begin{array}{lcl}
\chi_0^* = 1 & : & 1 \\
\chi_1^* & : & \zeta,\ \zeta^2,\ \zeta^4,\ \zeta^8 \\
\chi_2^* = \bar{\chi}_2^* & : & \zeta^3,\ \zeta^6,\ \zeta^{12},\ \zeta^9 \\
\chi_3^* = \bar{\chi}_3^* & : & \zeta^5,\ \zeta^{10} \\
\bar{\chi}_1^* & : & \zeta^7,\ \zeta^{14},\ \zeta^{13},\ \zeta^{11}
\end{array}$$

(1.5) implies that $(\chi_0^*, \chi_1^*, \chi_2^*, \chi_3^*, \bar{\chi}_1^*)$ or simply one representant of each class $(1, \zeta, \zeta^3, \zeta^5, \zeta^7)$ has the P_{15} property over $GF(2)$.

The inverses of χ_2^* and χ_3^* are χ_2^* and χ_3^*.

As proved in R. C. Bose (1), the set $(\zeta, \zeta^3, \zeta^5)$ has the P_6 property over $GF(2)$. Hence by 1.6 the set $(\bar{\zeta}, \bar{\zeta^3}, \bar{\zeta^5})$ has also the P_{10} property over $GF(2)$, i.e. $(\zeta^7, \zeta^3, \zeta^5)$

The character $\zeta^5 \quad : \quad c^a \longrightarrow x^{5a}$. Hence the values taken by ζ^5 are x^5, x^{10} and $x^{15} = 1$. Thus ζ^5 belongs to $GF(2^2)$ and the equivalence class to which it belongs, only contains two characters ζ^5 and ζ^{10}.

Example 2. Consider the Abelian group G, direct sum of the cyclic group of order 15 and of the cyclic group of order 3:

$G = G_{15} \oplus G_3$.

We have just seen that for G_{15} we can take $GF(2^4)$ for the field ;

x, the primitive root of $GF(2^4)$ is an 15^{th} primitive root of unity. Hence x^5 is an 3^{rd} primitive root of unity.

Thus the character of $\Sigma\ (G,2,4)$ are:

$$\zeta_1^u\ \zeta_2^v \quad : \quad (a_1,a_2) \longrightarrow x^{ua_1}\ x^{5va_2} = x^{ua_1 + 5va_2}$$

$u = 0, 1, \ldots, 14$ $a_1 = 0,1,\ldots,14$

$v = 0, 1, 2$ $\qquad a_2 = 0,1,2$

To the equivalence relation $\Phi(1)$ correspond the classes:

X_o^*	:	1
X_1^*	:	$\zeta_1, \zeta_1^2, \zeta_1^4, \zeta_1^8$
$X_2^* = \bar{X}_2^*$	:	ζ_2, ζ_2^2
$X_3^* = \bar{X}_3^*$	:	$\zeta_1^3, \zeta_1^6, \zeta_1^{12}, \zeta_1^9$
X_4^*	:	$\zeta_1\zeta_2, \zeta_1^2\ \zeta_2^2, \zeta_1^4\zeta_2, \zeta_1^8, \zeta_2^2$
X_5^*	:	$\zeta_1^2\zeta_2, \zeta_1^4\zeta_2^2, \zeta_1^8\zeta_2, \zeta_1\zeta_2^2$
X_6^*	:	$\zeta_1^3\zeta_2, \zeta_1^6\zeta_2^2, \zeta_1^{12}\zeta_2, \zeta_1^9\zeta_2^2$
$X_7^* = \bar{X}_7^*$	:	ζ_1^5, ζ_1^{10}
$\bar{X}_6^*$	:	$\zeta_1^3\zeta_2^2, \zeta_1^6\zeta_2, \zeta_1^{12}\zeta_2^2, \zeta_1^9\zeta_2$
$X_8^* = \bar{X}_8^*$	:	$\zeta_1^5\zeta_2, \zeta_1^{10}\zeta_2^2$
$\bar{X}_1^*$	:	$\zeta_1^7, \zeta_1^{14}, \zeta_1^{13}, \zeta_1^{11}$
$X_9^* = \bar{X}_9^*$	:	$\zeta_1^5\zeta_2^2, \zeta_1^{10}\zeta_2$
$\bar{X}_4^*$	:	$\zeta_1^7, \zeta_2, \zeta_1^{14}, \zeta_1^{13}\zeta_2, \zeta_1^{11}\zeta_2^2$
X_5^*	:	$\zeta_1^7\ \zeta_2^2, \zeta_1^{14}\zeta_2, \zeta_1^{13}\zeta_2^2, \zeta_1^{11}\zeta_2$

These 14 classes have the P_{45} property over GF(2).

Later we shall prove that $(1,\zeta_1,\zeta_1^2,\zeta_1^3,\zeta_1^4,\zeta_1^5,\zeta_2,\zeta_2^2,\zeta_1\zeta_2,\zeta_1\zeta_2^2,\zeta_1^2\zeta_2)$ has the P_6 property over $GF(2^4)$.

Hence the set of classes $(\chi_o^*,\chi_1^*,\chi_2^*,\chi_3^*,\chi_4^*,\chi_5^*,\chi_7^*)$ has the P_6 property over GF(2).

Hence by (1.6) the set of the inverse classes $(\chi_o^*,\bar{\chi}_1^*,\chi_2^*,\chi_3^*,\bar{\chi}_4^*,\bar{\chi}_5^*,\chi_7^*)$ has the P_6 property over GF(2) or if we pick one element from each of these classes:
the set $(1,\zeta_1^7,\zeta_2,\zeta_1^3,\zeta_1^7\zeta_2,\zeta_1^7\zeta_2^2,\zeta_1^5)$ has the P_6 property over GF(2).

-2-

If a character χ of Σ (G,m,p) belongs to an intermediate field $GF(p^e)$, $(GF(p^n) \subset GF(p^e) \subset GF(p^m))$, we will show, in this section, that the images $\chi(a)$ $(a \in G)$ can be represented isomorphically in a vector of length $\frac{e}{n} = e_1 = n^*$ (the number class of χ) with coordinates from $GF(p^n)$. We will call this vector $P(\chi(a), n^*)$.

Hence assuming that $(\chi_1,\chi_2,\dots,\chi_e)$ is a set of non-equivalent characters of Σ(G,m,p) having the P_d property over $GF(p^n)$, the substitution $\chi(a) \longrightarrow P(\chi(a), n^*)$ in the submatrix $(\chi_1,\dots,\chi_e)$ will yield to a matrix, with entries from $GF(p^n)$, having the P_d property.

We shall use the following theorem:

From C. C. Mac Duffee "An introduction to abstract algebra" page 109:

"Let $f(n) = x^n + a_1x^{n-1} + \dots + a_{n-1} x + a_n$ be a polynomial with coefficients in a field F and irreducible over F.

Let ρ be a root of this polynomial and consider the matrix:

$$R = \begin{bmatrix} 0\ 0 \dots 0 - a_n \\ 1\ 0 \dots 0 - a_{n-1} \\ 0\ 1 \dots 0 - a_{n-2} \\ \dots \quad 1 \quad \dots \\ 0\ 0 \dots 1 - a_1 \end{bmatrix}$$

Then the correspondence:

$$\alpha = c_o + c_1\,\rho + \dots + c_{n-1}\,\rho^{n-1} \longleftrightarrow c_o\,I + c_1 R + \dots + c_{n-1}\,R^{n-1} = A$$

is biunique and is an isomorphism under both addition and multiplication."

Denote the latter field by K. Hence:

Proposition 2.1. A set of k matrices from K are linearly dependent over F, if and only if, the first rows of these k matrices are linearly dependent over F.

"Only" is trivial. If the first rows of k matrices $A_1 A_2, \dots, A_k$ of K are linearly dependent, then there exist k elements of F_1: $\lambda_1, \lambda_2, \dots, \lambda_k$ such that $\lambda_1 A_1 + \lambda_2 A_2 + \dots + \lambda_k A_k$ is a matrix B whose first row is null.

But $B \in K$ and admits an inverse unless it is null. As having its first row null, B is singular and therefore is the null matrix.

Proposition 2.2. We can express this by saying: A set of k elements $\alpha_1, \alpha_2, \dots, \alpha_k$ of $F(\rho)$ are linearly independent over F, if and only if, the first rows of the corresponding matrices of K, $A_1, A_2, \dots, A_k$ in the isomorphism $\alpha \longleftrightarrow A$ are linearly independent.

Let us apply this result to our group characters from $\Sigma(G,p,m)$:

If n divides m, the field $GF(p^m)$ is an algebraic extension of $GF(p^n)$ of degree $m_1 = \frac{m}{n}$. Thus every element of $GF(p^m)$ can be isomorphically expressed as a matrix of order m_1 with entries from $GF(p^n)$.

In our character table $\Sigma(G,p,m)$, if a character χ belongs to an intermediate field $GF(p^e)$, all the images $\chi(a)$ $(a \in G)$ can be expressed as matrices of order $e_1 = \frac{e}{n} = n^*$ with entries from $GF(p^n)$, under the above isomorphism we shall denote:

$$\chi(a) \longleftrightarrow M\,(\chi\,(a),\, n^*)$$

(The order of these matrices $M(\chi(a), n^*)$ is equal to the degree of the extension of $GF(p^e)$ over $GF(p^n)$; that is, to n^*, the number of characters in the class χ^*).

The first rows of these matrices $M(\chi(a), n^*)$ will be denoted by $P(\chi(a), n^*)$.

(2.2) implies:

Proposition 2.3. If a set $(\chi_1, \chi_2, \ldots, \chi_k)$ of non-equivalent characters of $\Sigma(G,p,m)$ has the P_d property over $GF(p^n)$ (n divisor of m), then we can construct a matrix of g rows and $(n_1^* + n_2^* + \ldots + n_k^*)$ columns with entries from $GF(p^n)$ which has the P_d property.

Moreover the rank of this matrix is $(n_1^* + n_2^* + \ldots + n_k^*)$; n_i^* $(i = 1 \ldots k)$ being the number of characters in χ_i^*.

Indeed from (2.2) we deduce:

$\chi_i(a_1), \chi_i(a_2), \ldots, \chi_i(a_e)$ are linearly independent over $GF(p^n)$, if and only if, the e vectors of length n_i^*:

$P(\chi_i(a_1), n_i^*), P(\chi_i(a_2), n_i^*), \ldots, P(\chi_i(a_e), n_i^*)$ are linearly independent.

$(i = 1 \ldots k)$

Hence if we replace each element, $\chi_i(a)$, in the submatrix $(\chi_1, \chi_2, \ldots, \chi_k)$ of $\Sigma\,(G,m,p)$, by $P(\chi_i(a), n_i^*)$, we obtain a matrix with $(n_1^* + n_2^* + \ldots + n_k^*)$ columns and g rows and the P_d property is preserved.

Furthermore this matrix is of rank $(n_1^* + n_2^* + \ldots + n_k^*)$. For if we take all the character classes $(\chi_1^*, \chi_2^*, \ldots, \chi_{g^*}^*)$ and pick one representant from each class $(\chi_1, \chi_2, \ldots, \chi_{g^*})$, by (1.5) the matrix $(\chi_1, \chi_2, \ldots, \chi_{g^*})$ has the P_g property over $GF(p^n)$.

Hence if we replace each element $\chi_i(a)$ of this matrix by $P(\chi_i(a),n_i^*)$, we will get a non-singular square matrix of order g, since $n_1^* + n_2^* + \dots + n_g^* = g$.

This implies that the rank of the matrix $(\chi_1,\chi_2,\dots,\chi_k)$ after having made the substitution $\chi_i(a) \longrightarrow P(\chi_i(a), n_i^*)$, is $(n_1^* + \dots + n_k^*)$, which is the number of the columns.

-3-

We can now apply these results to cyclic groups.

We so obtain a reformulation of the results of Bose and Ray-Chaudhuri [1] and [2] in the general case. The result of Peterson [4] on the number of columns of the Bose-Chaudhuri matrices having the P_{2t} property over GF(2) is also being generalized and the present proposition follows:

Proposition 3.1. Let G be a cyclic group of order h, p a prime number not dividing h, m the order of p in the residue system modulo h and n a divisor of m.

Then for d given, we can construct a matrix of h rows and R(h,d,n) columns with entries from $GF(p^n)$ having the P_d property.

R(h,d,n) is given by the number of residue systems mod h among the integers:

$q^j u \ (u = 1,2,\dots,d \ ; \ j \geq 0) \ q = p^n$

Under these assumptions x^c is an h^{th} primitive root of unity in $GF(p^m)$, where $c = \frac{p^m-1}{c}$ and x is a primitive root of $GF(p^m)$.

Hence the group $\Sigma(G_h,p,m)$ consists of

$\chi_u = \zeta^u: \ b^a \longrightarrow x^{ca}$

$u=0,1,\dots,(h-1) \ a=0,1,\dots,(h-1)$

The submatrix $(\chi_1,\chi_2,\dots,\chi_d)$ of $\Sigma(G_h,p,m)$ has the P_d property since any set of d rows $b^{a_1}, b^{a_2}, \dots, b^{a_d}$ yields to a square matrix:

$$\begin{bmatrix} x^{ca_1} & x^{2ca_1} & \cdots & x^{dca_1} \\ x^{ca_2} & x^{2ca_2} & \cdots & x^{dca_2} \\ \cdots & & \cdots & \\ x^{ca_d} & x^{2ca_d} & \cdots & x^{dca_d} \end{bmatrix}$$

which is non-singular, since its determinant is a Vandermonde determinant.

Hence the set $(\chi^*_i, \chi^*_{i_2}, \ldots, \chi^*_{i_{d^*}})$ obtained from $(\chi_1, \chi_2, \ldots, \chi_d)$ by retaining only one representant of each class has the P_d property over $GF(p^n)$ by (1.3).

But the congruence:

$$\chi_i \equiv \chi_j \text{ modulo } \Phi(n)$$

means that
$$i \equiv j\, q^k(h) \text{ for a certain } k$$
$$j \equiv i\, q^{k'}(h) \text{ for a certain } k'.$$

Hence the two sets $iq^u \quad u = 0,1,\ldots,m_1-1$

and $\quad j\, q^v \quad v = 0,1,\ldots,m_1-1$

are the same.

Thus the numder d^* of the class characters $(\chi^*_{i_1}, \chi^*_{i_2}, \ldots, \chi^*_{i_{d^*}})$ is equal to the number of distinct sets among the d sets: $(jq^u; u \geq o)$ $j=1,2,\ldots,d$ these numbers taken modulo h.

Now if we make the substitution $\chi^*_i(a) \longrightarrow P(\chi^*_i(a); n^*_i)$ $(i = i_1, i_2, \ldots, i_{d^*})$, $a \in G_h$, in the submatrix $(\chi^*_{i_1}, \chi^*_{i_2}, \ldots, \chi^*_{i_{d^*}})$, the P_d property is preserved by (2.3) and the number of columns we obtain is equal to: $n^*_{i_1} + n^*_{i_2} + \ldots + n^*_{i_{d^*}}$, the number of different residue systems modulo h among: $\quad q^j u \quad (u = 1,2,\ldots,d;\ j \geq 0)$ since by (1.7), n^*_i is equal to the number of different distinct residue systems mod h among $iq^u \quad u = 0,1,\ldots,m_1-1$.

4.

In this section we shall present, up to $d = 6$, sets of characters of an Abelian group which have the P_d-property. Hence using the techniques of section 1 and 2, we can construct matrices having the P_d-property with entries from some Galois field of characteristic p, when p does not divide the order of the group.

Let G by an Abelian group whose invariants are $(h_1, h_2, \ldots, h_r)$ and let $\zeta_1^{u_1}\zeta_2^{u_2} \ldots \zeta_r^{u_r}$ $(0 \leq u_1 \leq h_1 - 1,\ 0 \leq u_2 \leq h_2 - 1, \ldots, 0 \leq u_r \leq h_r - 1)$ be its $g = h_1 h_2 \ldots h_r$ characters.

We have just seen that when $r = 1$ (cyclic group), the set $(\zeta, \zeta^2, \ldots, \zeta^d)$ had the P_d-property.

What can we say when the number of invariants is greater than 1?

We shall use the same method: in order to prove that the set $(\chi_1, \chi_2, \ldots, \chi_e)$ of characters of G has the P_d-property, we shall show that in the submatrix of Σ formed by the e columns $(\chi_1, \chi_2, \ldots, \chi_e)$ and any d rows, there always exists a square matrix of order d, which is non-singular.

We make the convention that any character $\zeta_1^{u_1}\zeta_2^{u_2} \ldots \zeta_r^{u_r}$, in which an exponent u_i is greater than h_i, vanishes. Moreover, we shall denote by P_i the function : $a \rightarrow a_i = P_i(a)$ (a being an element of G, $a = (a_1, a_2, \ldots, a_r)$).

(4.1) <u>The set $(1, \zeta_1, \zeta_2, \ldots, \zeta_r)$ has the P_2-property.</u>

Consider two elements $a_1 = (a_{11} a_{12} \ldots a_{1r})$ and $a_2 = (a_{21} a_{22} \ldots a_{2r})$ of G. They differ at least by one coordinate, the <u>ith</u> (say), i.e. $a_{1i} \neq a_{2i}$. Then the submatrix $(1, \zeta_i)$ is : $\begin{pmatrix} 1 & \zeta_i^{a_{1i}} \\ 1 & \zeta_i^{a_{2i}} \end{pmatrix}$ which is non-singular.

(4.2) The set $(\zeta_1,\zeta_1^{\,2},\ \zeta_2,\zeta_2^{\,2},\ldots,\zeta_p,\zeta_p^{\,2})$ has the P_2-property.

Again if the ith coordinates of a_1 and a_2 are different, the submatrix $(\zeta_i,\zeta_i^{\,2})$ is: $\begin{pmatrix} \zeta_i^{a_{1i}} & \zeta_i^{2a_{1i}} \\ \zeta_i^{a_{2i}} & \zeta_i^{2a_{2i}} \end{pmatrix}$ which is non-singular.

(4.3) The set $(1,\zeta_1,\zeta_1^{\,2},\ \zeta_2,\zeta_2^{\,2},\ldots,\zeta_r,\zeta_r^{\,2})$ has the P_3-property.

Consider three elements of G:

$a_1=(a_{11}a_{12}\ldots a_{1r})$ $\quad a_2=(a_{21}a_{22}\ldots a_{2r})$ $\quad a_3=(a_{31}a_{32}\ldots a_{3r})$

If there exists a coordinate i, in which they all differ, we pick the subset $(1,\zeta_i,\zeta_i^{\,2})$ and the corresponding submatrix is:

$$\begin{pmatrix} 1 & \zeta_i^{a_{1i}} & \zeta_i^{2a_{1i}} \\ 1 & \zeta_i^{a_{2i}} & \zeta_i^{2a_{2i}} \\ 1 & \zeta_i^{a_{3i}} & \zeta_i^{2a_{3i}} \end{pmatrix} \qquad \text{which is non-singular.}$$

If it does not happen, there exists, however, a coordinate i in which a_1 and a_2 differ and also a coordinate $k \neq i$ in which a_1 and a_3 differ. We then choose the subset $(1,\zeta_i,\zeta_k)$ and the corresponding submatrix is:

$$\begin{pmatrix} 1 & \zeta_i^{a_{1i}} & \zeta_k^{a_{1k}} \\ 1 & \zeta_i^{a_{2i}} & \zeta_k^{a_{2k}} \\ 1 & \zeta_i^{a_{1i}} & \zeta_k^{a_{3k}} \end{pmatrix}$$

Its determinant is: $\pm(\zeta_k^{a_{3k}} - \zeta_k^{a_{1k}})(\zeta_i^{a_{2i}} - \zeta_i^{a_{1i}})$ which is non-null since $a_{2i} \neq a_{1i}$ and $a_{3k} \neq a_{1k}$.

Proposition 4.4

The set $(1,\zeta_i,\zeta_i^2,\zeta_i^3;\ \zeta_i\zeta_j;\ i=1,2,\ldots,r \text{ and } i \neq j)$ has the P_4-property.

Let $a_1a_2a_3a_4$ be 4 distinct elements of G. We have 4 cases to consider:

a) The $k^{\underline{th}}$ coordinates $a_{1k},a_{2k},a_{3k},a_{4k}$, of these four elements are distinct.

But then from the set $(1,\zeta_k,\zeta_k^2,\zeta_k^3)$ we obtain matrix:

$$\begin{array}{cc} & \begin{array}{cccc} 1, & \zeta_k & \zeta_k^2 & \zeta_k^3 \end{array} \\ \begin{array}{c} a_{1k} \\ a_{2k} \\ a_{3k} \\ a_{4k} \end{array} & \begin{pmatrix} 1 & \zeta_k^{a_{1k}} & \zeta_k^{2a_{1k}} & \zeta_k^{3a_{1k}} \\ 1 & \zeta_k^{a_{2k}} & \zeta_k^{2a_{2k}} & \zeta_k^{3a_{2k}} \\ 1 & \zeta_k^{a_{3k}} & \zeta_k^{2a_{3k}} & \zeta_k^{3a_{3k}} \\ 1 & \zeta_k^{a_{4k}} & \zeta_k^{2a_{4k}} & \zeta_k^{3a_{4k}} \end{pmatrix} \end{array}$$

which is non-singular (Vandermonde matrix).

b) There exists a coordinate k for which three elements, (say) $a_1\ a_2\ a_3$, have their coordinates distinct and the fourth one a_4 has its $k^{\underline{th}}$ coordinate a_{4k} equal to a_{3k} (say). Then there exists another coordinate i such that $P_i(a_3) = a_{3i} \neq a_{4i} = P_i(a_4)$.

In this case, the subset $(1,\zeta_k,\zeta_k^2,\zeta_i)$ gives the submatrix:

$$\begin{array}{ccc} & & \begin{array}{cccc} 1 & \zeta_k & \zeta_k^2 & \zeta_i \end{array} \\ \begin{array}{c} a_{1k} \\ a_{2k} \\ a_{3k} \\ a_{3k} \end{array} & \begin{array}{c} * \\ * \\ a_{3i} \\ a_{4i} \end{array} & \begin{pmatrix} 1 & \zeta_k^{a_{1k}} & \zeta_k^{2a_{1k}} & * \\ 1 & \zeta_k^{a_{2k}} & \zeta_k^{2a_{2k}} & * \\ 1 & \zeta_k^{a_{3k}} & \zeta_k^{2a_{3k}} & \zeta_i^{a_{3i}} \\ 1 & \zeta_k^{a_{3k}} & \zeta_k^{2a_{3k}} & \zeta_i^{a_{4i}} \end{pmatrix} \end{array}$$

and the determinant of this matrix is:

$$\pm\left(\zeta_i^{a_{4i}} - \zeta_i^{a_{3i}}\right) \begin{vmatrix} 1 & \zeta_k^{a_{1k}} & \zeta_k^{2a_{1k}} \\ 1 & \zeta_k^{a_{2k}} & \zeta_k^{2a_{2k}} \\ 1 & \zeta_k^{a_{3k}} & \zeta_k^{2a_{3k}} \end{vmatrix} \neq 0$$

c) In k, 3 coordinates are equal and the fourth one is different, or:

$$P_k(a_1) = P_k(a_2) = P_k(a_3) = a_{1k}$$

and

$$P_k(a_4) = a_{4k} \neq a_{1k} \quad .$$

Then there exists another coordinate i with $P_i(a_1) = a_{1i} \neq a_{2i} = P_i(a_2)$.

If a_{1i}, a_{2i} and $a_{4i} = P_i(a_4)$ are distinct, then we are in the case b). Hence suppose a_{4i} is equal to a_{1i} (a_1 and a_2 play the same role). Now if $a_{3i} = P_i(a_3)$ is different from a_{1i} or a_{2i} we are again in the case b). Thus we are left with: $P_i(a_3) = a_{1i}$ and then there exists another coordinate j for which $P_j(a_3) = a_{3j} \neq a_{1j} = P_j(a_1)$ or $P_i(a_3) = a_{2i}$ and then there exists another coordinate l for which $P_l(a_3) = a_{3l} \neq a_{2l} = P_l(a_2)$.

In the first case the subset $(1, \zeta_k, \zeta_i, \zeta_j)$ gives the submatrix:

$$\begin{matrix} a_{1k} & a_{1i} & a_{1j} \\ a_{1k} & a_{2i} & * \\ a_{1k} & a_{1i} & a_{3j} \\ a_{4k} & a_{1i} & * \end{matrix} \qquad \begin{array}{c} \begin{matrix} 1 & \zeta_k & \zeta_i & \zeta_j \end{matrix} \\ \begin{pmatrix} 1 & \zeta_k^{a_{1k}} & \zeta_i^{a_{1i}} & \zeta_j^{a_{1j}} \\ 1 & \zeta_k^{a_{1k}} & \zeta_i^{a_{2i}} & * \\ 1 & \zeta_k^{a_{1k}} & \zeta_i^{a_{1i}} & \zeta_j^{a_{3j}} \\ 1 & \zeta_k^{a_{4k}} & \zeta_i^{a_{1i}} & * \end{pmatrix} \end{array}$$

which is non-singular. Its determinant is equal to:

$$\pm(\zeta_k^{a_{1k}} - \zeta_k^{a_{4k}})(\zeta_i^{a_{2i}} - \zeta_i^{a_{1i}})(\zeta_j^{a_{1j}} - \zeta_j^{a_{3j}}) \neq 0 \; .$$

In the second case the subset $(1, \zeta_k, \zeta_i, \zeta_1)$ gives the submatrix:

$$\begin{array}{cc} & \begin{matrix} 1 & \zeta_k & \zeta_i & \zeta_1 \end{matrix} \\ \begin{matrix} a_{1k} & a_{1i} & * \\ a_{1k} & a_{2i} & a_{21} \\ a_{1k} & a_{2i} & a_{31} \\ a_{1k} & a_{1i} & * \end{matrix} & \begin{pmatrix} 1 & \zeta_k^{a_{1k}} & \zeta_i^{a_{1i}} & * \\ 1 & \zeta_k^{a_{1k}} & \zeta_i^{a_{2i}} & \zeta_1^{a_{21}} \\ 1 & \zeta_k^{a_{1k}} & \zeta_i^{a_{2i}} & \zeta_1^{a_{31}} \\ 1 & \zeta_k^{a_{4k}} & \zeta_i^{a_{1i}} & * \end{pmatrix} \end{array}$$

Again its determinant is equal to: $(\zeta_k^{a_{4k}} - \zeta_k^{a_{1k}})(\zeta_i^{a_{2i}} - \zeta_i^{a_{1i}})(\zeta_1^{a_{21}} - \zeta_1^{a_{31}}) \neq 0.$

d) We are left with the case:

$$\text{in } k, \quad P_k(a_1) = P_k(a_2) = a_{1k}$$

$$\text{and} \quad P_k(a_3) = P_k(a_4) = a_{3k} \quad .$$

But there exists another coordinate j such that $P_j(a_1) = a_{1j}$ is different from $a_{2j} = P_j(a_2)$.

If one of the coordinates $P_j(a_3)$ or $P_j(a_4)$ is different from a_{1j} and a_{2j} we are in the case a) or the case b). Also if $P_j(a_3)$ and $P_j(a_4)$ are both equal to one of the coordinates a_{ij} or a_{2j} we are in the case c). Thus we only have to see the case where

$$P_j(a_3) = a_{ij} \quad \text{and} \quad P_j(a_4) = a_{2j}$$

(a_3 and a_4 have a symmetric role).

Then the subset $(1, \zeta_k, \zeta_j, \zeta_j \zeta_k)$ gives:

$$
\begin{array}{cc|cccc}
 & & 1 & \zeta_k & \zeta_j & \zeta_j\zeta_k \\
a_{1k} & a_{1j} & & & & \\
a_{1k} & a_{2j} & & & & \\
a_{3k} & a_{1j} & & & & \\
a_{3k} & a_{2j} & & & &
\end{array}
\qquad
\begin{pmatrix}
1 & \zeta_k^{a_{1k}} & \zeta_j^{a_{1j}} & \zeta_k^{a_{1k}}\zeta_j^{a_{1j}} \\
1 & \zeta_k^{a_{1k}} & \zeta_j^{a_{2j}} & \zeta_k^{a_{1k}}\zeta_j^{a_{2j}} \\
1 & \zeta_k^{a_{3k}} & \zeta_j^{a_{1j}} & \zeta_k^{a_{3k}}\zeta_j^{a_{1j}} \\
1 & \zeta_k^{a_{3k}} & \zeta_j^{a_{2j}} & \zeta_k^{a_{3k}}\zeta_j^{a_{2j}}
\end{pmatrix}
$$

Its determinant is equal to:

$$\pm(\zeta_j^{a_{2j}} - \zeta_j^{a_{1j}})^2 \; (\zeta_k^{a_{3k}} - \zeta_k^{a_{1k}})^2 \neq 0 \quad .$$

We shall now continue, but only with Abelian group with two invariants: $G = G_{h_1} \oplus G_{h_2} \quad h_2/h_1 \quad$ and $h_1 \geq 3$.

The characters will be denoted by $\zeta^u \eta^v$

$$u = 0,1,\ldots,h_1 - 1$$
$$v = 0,1,\ldots,h_2 - 1 \; .$$ Then

Proposition 4.5

The set $(1,\zeta,\zeta^2,\zeta^3,\zeta^4,\eta,\eta^2,\eta^3,\eta^4,\zeta\eta)$ has the P_5-property.

Consider 5 elements of G:

$a_1=(a_{11},a_{12}) \quad a_2=(a_{21},a_{22}) \quad a_3=(a_{31},a_{32}) \quad a_4=(a_{41},a_{42}) \quad a_5=(a_{51},a_{52})$

We note that there always exists a coordinate in which at least 3 elehave distinct coordinates. Let us make the reasoning on the first coordinate.

We have 4 cases to consider:

1. $a_{11}\ a_{21}\ a_{31}\ a_{41}\ a_{51}$ all distinct
2. $a_{11}\ a_{21}\ a_{31}\ a_{41}$ distinct and $a_{51} = a_{41}$
3. $a_{11}\ a_{21}\ a_{31}$ distinct and $a_{51} = a_{41} = a_{31}$
4. $a_{11}\ a_{21}\ a_{31}$ distinct and $a_{41} = a_{31}$ and $a_{51} = a_{21}$

In case 1, the subset $(1,\zeta,\zeta^2,\zeta^3,\zeta^4)$ gives a non-singular matrix .

In case 2, the subset $(1,\zeta,\zeta^2,\zeta^3,\eta)$ will give the submatrix:

$$
\begin{array}{cc c}
 & & \begin{array}{ccccc} 1 & \zeta & \zeta^2 & \zeta^3 & \eta \end{array} \\
\begin{array}{c} a_{11} \\ a_{21} \\ a_{31} \\ a_{41} \\ a_{51} \end{array} & \begin{array}{c} * \\ * \\ * \\ a_{42} \\ a_{52} \end{array} & \begin{pmatrix}
1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} & * \\
1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} & * \\
1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} & * \\
1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \eta^{a_{42}} \\
1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \eta^{a_{52}}
\end{pmatrix}
\end{array}
$$

and its determinant is equal to:

$$
\pm\,(\eta^{a_{52}} - \eta^{a_{42}}) \begin{vmatrix}
1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} \\
1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} \\
1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} \\
1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}}
\end{vmatrix}
$$

which is different from 0 since $a_{52} \neq a_{42}$ and $a_{11}a_{21}a_{31}a_{41}$ all different.

In case 3, the subset $(1,\zeta,\zeta^2,\eta,\eta^2)$ gives the submatrix:

$$
\begin{array}{cc c}
 & & \begin{array}{ccccc} 1 & \zeta & \zeta^2 & \eta & \eta^2 \end{array} \\
\begin{array}{c} a_{11} \\ a_{21} \\ a_{31} \\ a_{31} \\ a_{31} \end{array} & \begin{array}{c} * \\ * \\ a_{32} \\ a_{42} \\ a_{52} \end{array} & \begin{pmatrix}
1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & * & * \\
1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & * & * \\
1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{32}} & \eta^{2a_{32}} \\
1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{42}} & \eta^{2a_{42}} \\
1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{52}} & \eta^{2a_{52}}
\end{pmatrix}
\end{array}
$$

and its determinant is: $\begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} \end{vmatrix} \cdot \begin{vmatrix} 1 & \eta^{a_{32}} & \eta^{2a_{32}} \\ 1 & \eta^{a_{42}} & \eta^{2a_{42}} \\ 1 & \eta^{a_{52}} & \eta^{2a_{52}} \end{vmatrix} \neq 0$

since a_{11} a_{21} a_{31} are all different and also a_{32} a_{42} and a_{52}.

In the latter case we pick the subset $(1,\zeta,\zeta^2,\eta,\zeta\eta)$ and we have

$$\begin{array}{cc} & \\ a_{11} & * \\ a_{21} & a_{22} \\ a_{31} & a_{32} \\ a_{31} & a_{42} \\ a_{21} & a_{52} \end{array} \quad \begin{array}{c} \begin{array}{ccccc} 1 & \zeta & \zeta^2 & \eta & \zeta\eta \end{array} \\ \begin{pmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & * & * \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \eta^{a_{22}} & \zeta^{a_{21}}\eta^{a_{22}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{32}} & \zeta^{a_{31}}\eta^{a_{32}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{42}} & \zeta^{a_{31}}\eta^{a_{42}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \eta^{a_{52}} & \zeta^{a_{21}}\eta^{a_{52}} \end{pmatrix} \end{array}$$

Its determinant is equal to:

$$\pm(\zeta^{a_{31}} - \zeta^{a_{21}})(\eta^{a_{42}} - \eta^{a_{32}})(\eta^{a_{52}} - \eta^{a_{22}}) \begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} \end{vmatrix} \neq 0$$

since a_{11} a_{21} a_{31} are all different and also $a_{42} \neq a_{32}$ and $a_{52} \neq a_{22}$.

<u>Proposition 4.6</u>

<u>The set $(1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5,\eta,\eta^2,\eta^3,\eta^4,\eta^5,\zeta\eta,\zeta\eta^2,\zeta^2\eta)$ has the P_6-property.</u>

Let $a_1 a_2 a_3 a_4 a_5 a_6$ be 6 distinct elements of G. We remark that there always exists a coordinate in which at least 3 elements have distinct coordinates. Let us make the reasoning on the first coordinate.

Thus we only have 6 cases

1. $a_{11}\ a_{21}\ a_{31}\ a_{41}\ a_{51}\ a_{61}$ all distinct
2. $a_{11}\ a_{21}\ a_{31}\ a_{41}\ a_{51}$ distinct and $a_{61} = a_{51}$
3. $a_{11}\ a_{21}\ a_{31}\ a_{41}$ distinct and $a_{61} = a_{51} = a_{41}$
4. $a_{11}\ a_{21}\ a_{31}\ a_{51}$ distinct and $a_{61} = a_{51}$ and $a_{41} = a_{31}$
5. $a_{11}\ a_{21}\ a_{41}$ distinct and $a_{31} = a_{21}$
6. $a_{11}\ a_{31}\ a_{51}$ distinct and $a_{21} = a_{11}\quad a_{41} = a_{31}\quad a_{61} = a_{51}$

In case 1, the set $(1,\zeta,\zeta^2,\zeta^3,\zeta^4,\zeta^5)$ gives a non-singular matrix (of Vandermonde) since all the coordinates are different.

In case 2 the set $(1,\zeta,\zeta^2,\zeta^3,\zeta^4,\eta)$ gives:

$$\begin{array}{cc} a_{11} & * \\ a_{21} & * \\ a_{31} & * \\ a_{41} & * \\ a_{51} & a_{52} \\ a_{51} & a_{62} \end{array} \begin{pmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} & \zeta^{4a_{11}} & * \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} & \zeta^{4a_{21}} & * \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} & \zeta^{4a_{31}} & * \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \zeta^{4a_{41}} & * \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \zeta^{3a_{51}} & \zeta^{4a_{51}} & \eta^{a_{52}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \zeta^{3a_{51}} & \zeta^{4a_{51}} & \eta^{a_{62}} \end{pmatrix}$$

its determinant is equal to:

$$(\eta^{a_{62}} - \eta^{a_{52}}) : \begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} & \zeta^{4a_{11}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} & \zeta^{4a_{21}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} & \zeta^{4a_{31}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \zeta^{4a_{41}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \zeta^{3a_{51}} & \zeta^{4a_{51}} \end{vmatrix}$$

different from zero by our hypothesis.

In case 3, we take the set: $(1,\zeta,\zeta^2,\zeta^3,\eta,\eta^2)$ and we get the submatrix:

$$\begin{array}{cc} a_{11} & * \\ a_{21} & * \\ a_{31} & * \\ a_{41} & a_{42} \\ a_{41} & a_{52} \\ a_{41} & a_{62} \end{array} \begin{pmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} & * & * \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} & * & * \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} & * & * \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \eta^{a_{42}} & \eta^{2a_{42}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \eta^{a_{52}} & \eta^{2a_{52}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} & \eta^{a_{62}} & \eta^{2a_{62}} \end{pmatrix}$$

and its determinant is equal to:

$$\begin{vmatrix} 1 & \eta^{a_{42}} & \eta^{2a_{42}} \\ 1 & \eta^{a_{52}} & \eta^{2a_{52}} \\ 1 & \eta^{a_{62}} & \eta^{2a_{62}} \end{vmatrix} \cdot \begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \zeta^{3a_{41}} \end{vmatrix} \neq 0$$

since $a_{11}\ a_{21}\ a_{31}\ a_{41}$ are all different and also necessarily $a_{42}\ a_{52}\ a_{62}$.

In case 4, we take the set $(1,\zeta,\zeta^2,\zeta^3,\eta,\zeta\eta)$ and we obtain the submatrix:

$$\begin{array}{cc} a_{11} & * \\ a_{21} & * \\ a_{31} & a_{32} \\ a_{31} & a_{42} \\ a_{51} & a_{52} \\ a_{51} & a_{62} \end{array} \begin{pmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} & * & * \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} & * & * \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} & \eta^{a_{32}} & \zeta^{a_{31}}\eta^{a_{32}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} & \eta^{a_{42}} & \zeta^{a_{31}}\eta^{a_{42}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \zeta^{3a_{51}} & \eta^{a_{52}} & \zeta^{a_{51}}\eta^{a_{52}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \zeta^{3a_{51}} & \eta^{a_{62}} & \zeta^{a_{51}}\eta^{a_{62}} \end{pmatrix}$$

Its determinant is equal to:

$$\pm(\eta^{a_{42}} - \eta^{a_{32}})(\eta^{a_{62}} - \eta^{a_{52}})(\zeta^{a_{51}} - \zeta^{a_{31}}) \begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \zeta^{3a_{11}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \zeta^{3a_{21}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \zeta^{3a_{31}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \zeta^{3a_{51}} \end{vmatrix}$$

which is different from zero since $a_{11}\ a_{21}\ a_{31}\ a_{51}$ are all different and $a_{42} \neq a_{32}$ and $a_{62} \neq a_{52}$.

In case 5, the set $(1,\zeta,\zeta^2,\eta,\eta^2,\zeta\eta)$ is chosen and the following matrix is obtained:

$$\begin{array}{cc} a_{11} & * \\ a_{21} & a_{22} \\ a_{21} & a_{32} \\ a_{41} & a_{42} \\ a_{41} & a_{52} \\ a_{41} & a_{62} \end{array} \begin{pmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & * & * & * \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \eta^{a_{22}} & \eta^{2a_{22}} & \zeta^{a_{21}}\eta^{a_{22}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} & \eta^{a_{32}} & \eta^{2a_{32}} & \zeta^{a_{21}}\eta^{a_{32}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \eta^{a_{42}} & \eta^{2a_{42}} & \zeta^{a_{41}}\eta^{a_{42}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \eta^{a_{52}} & \eta^{2a_{52}} & \zeta^{a_{41}}\eta^{a_{52}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} & \eta^{a_{62}} & \eta^{2a_{62}} & \zeta^{a_{41}}\eta^{a_{62}} \end{pmatrix}$$

Its determinant is equal to:

$$\pm(\eta^{a_{32}} - \eta^{a_{22}})(\eta^{a_{52}} - \eta^{a_{42}})(\eta^{a_{62}} - \eta^{a_{42}})(\eta^{a_{62}} - \eta^{a_{52}})(\zeta^{a_{41}} - \zeta^{a_{21}}) \begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} \\ 1 & \zeta^{a_{21}} & \zeta^{2a_{21}} \\ 1 & \zeta^{a_{41}} & \zeta^{2a_{41}} \end{vmatrix} \neq 0$$

$a_{11}\ a_{21}\ a_{41}$ are all different

$a_{42}\ a_{52}\ a_{62}$ ——————————

$a_{32} \neq a_{22}$

In case 6 we take the set $(1,\zeta,\zeta^2,\eta,\eta\zeta,\eta\zeta^2)$ and we have:

$$\begin{array}{cc} a_{11} & a_{12} \\ a_{11} & a_{22} \\ a_{31} & a_{32} \\ a_{31} & a_{42} \\ a_{51} & a_{52} \\ a_{51} & a_{62} \end{array} \begin{pmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \eta^{a_{12}} & \eta^{a_{12}}\zeta^{a_{11}} & \eta^{a_{12}}\zeta^{2a_{11}} \\ 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} & \eta^{a_{22}} & \eta^{a_{22}}\zeta^{a_{11}} & \eta^{a_{22}}\zeta^{2a_{11}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{32}} & \eta^{a_{32}}\zeta^{a_{31}} & \eta^{a_{32}}\zeta^{2a_{31}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} & \eta^{a_{42}} & \eta^{a_{42}}\zeta^{a_{31}} & \eta^{a_{42}}\zeta^{2a_{31}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \eta^{a_{52}} & \eta^{a_{52}}\zeta^{a_{51}} & \eta^{a_{52}}\zeta^{2a_{51}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} & \eta^{a_{62}} & \eta^{a_{62}}\zeta^{a_{51}} & \eta^{a_{62}}\zeta^{2a_{51}} \end{pmatrix}$$

Its determinant is equal to:

$$\pm(\eta^{a_{22}}-\eta^{a_{12}})(\eta^{a_{42}}-\eta^{a_{32}})(\eta^{a_{62}}-\eta^{a_{52}}) \begin{vmatrix} 1 & \zeta^{a_{11}} & \zeta^{2a_{11}} \\ 1 & \zeta^{a_{31}} & \zeta^{2a_{31}} \\ 1 & \zeta^{a_{51}} & \zeta^{2a_{51}} \end{vmatrix}^2 \neq 0$$

since a_{11} a_{31} a_{51} are all distinct & $a_{22} \neq a_{12}$ $a_{42} \neq a_{32}$ $a_{62} \neq a_{52}$.

Let us conclude by an application and an example.

<u>Proposition 4.7</u>

<u>If $g = (2^{ee_1}-1)(2^e-1)$, we can construct a matrix of g rows and $e(e_1+1)$ columns with entries from GF(2) which has the P_2-property.</u>

Consider the Abelian group $G = (h_1,h_2)$, $h_1 = 2^{ee_1}-1$, $h_2 = 2^e-1$. Then if x is a primitive root of $GF(2^{ee_1})$, the character of $\Sigma\ (G,2,ee_1)$ are:

$$\zeta^u\eta^v : (a_1,a_2) \longrightarrow x^{ua_1+e_1va_2}$$

$u = 0,1,\ldots,h_1-1$

$v = 0,1,\ldots,h_2-1$

To $n = 1$ corresponds the equivalence relation $\Phi(1)$ and as $\alpha \longrightarrow \alpha^2$ is an automorphism of GF(2), we have:

$$\zeta \equiv \zeta^2 \mod \Phi(1)$$
$$\eta \equiv \eta^2 \mod \Phi(1) \quad .$$

Hence by (1.2) and (4.2) the set (ζ,η) has the P_2-property over $GF(2)$. On the other hand ζ belongs to $GF(2^{ee_1})$ and η to $GF(2^e)$. Hence by (2.3) we can construct a matrix, with entries from GF(2), of g rows and $n_1^* + n_2^* = ee_1 + e = e(e_1 + 1)$ columns, which has the P_2-property.

Moreover since $2^{e_1e+e-1} - 1 < (2^{e_1e} - 1)(2^e - 1) < 2^{e_1e+e} - 1$ for $e \geq 2$, the matrix obtained from the Bose-Chaudhuri construction [1] page 73, by representing each non-null element of $GF(2^{e(e_1+1)})$ as an $e(e_1+1)$-vector over GF(2) and deleting $(2^{e(e_1+1)}-1) - (2^{e_1e}-1)(2^e-1)$ rows, has as many columns, that is $e(e_1+1)$.

Let us work out the group $G = (3,3)$

$$(h_1 = 3,\ h_2 = 3)$$

$p = 2$ has the order $m = 2$ in the residue system modulo 3:

$$2^2 = 4 \equiv 1(3) \quad .$$

Hence if x is a primitive root of $GF(2^2)$, the characters of $\Sigma(G,2,2)$ are:

$$\zeta^u\eta^v \qquad (a_1,a_2) \longrightarrow x^{ua_1+va_2}$$

$$\begin{array}{ll} u=0,1,2 & a_1=0,1,2 \\ v=0,1,2 & a_2=0,1,2 \end{array}$$

Now $GF(2^2)$ has only GF(2) as a subfield (n=1). Corresponding to the equivalence relation $\Phi(1)$, the classes of characters are:

$$\begin{array}{ll} X_0^* : & 1 \\ X_1^* : & \zeta,\ \zeta^2 \\ X_2^* : & \eta.\ \eta^2 \\ X_3^* : & \zeta\eta,\ \zeta^2\eta^2 \\ X_4^* : & \zeta\eta^2, \zeta^2\eta \end{array}$$

By (1.5) these five classes have the P_9-property over GF(2) i.e. if we pick one character from each class $(1,\zeta,\eta,\zeta\eta,\zeta\eta^2)$ the obtained matrix:

$$\begin{array}{c|c} & \begin{array}{ccccc} 1 & \zeta & \eta & \zeta\eta & \zeta\eta^2 \end{array} \\ \begin{array}{c} (0,0) \\ (1,0) \\ (2,0) \\ (0,1) \\ (1,1) \\ (2,1) \\ (0,2) \\ (1,2) \\ (2,2) \end{array} & \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & x & 1 & x & x \\ 1 & x^2 & 1 & x^2 & x^2 \\ 1 & 1 & x & x & x^2 \\ 1 & x & x & x^2 & 1 \\ 1 & x^2 & x & 1 & x \\ 1 & 1 & x^2 & x^2 & x \\ 1 & x & x^2 & 1 & x^2 \\ 1 & x^2 & x^2 & x & 1 \end{pmatrix} \end{array}$$

has the P_9-property over GF(2).

Now the matrix representation of $GF(2^2)$ of section 2 is:

$$x \rightarrow \binom{01}{11} \qquad x^2 \rightarrow \binom{11}{10} \qquad x^3 = 1 \rightarrow \binom{10}{01} \quad ;$$

if we consider $GF(2^2)$ as the algebraic extension of GF(2) by the addition of a root of the polynomial : $x^2 + x + 1$.

Hence if, in the above matrix, we make the substitution:

$$P: \quad X_i(a) \longrightarrow P(X_i(a),\ n_i^*\ ) \qquad \text{(section 2)}$$

the first column will remain alike and the elements of the other columns will be replaced by a 2-vector over GF(2), namely the first rows of the matrices corresponding to 1, x and x^2 or

$$1 \rightarrow (1,0) \qquad x \rightarrow (0,1) \qquad x^2 \rightarrow (1,1)$$

Then we get the non-singular matrix of order 9 with entries from GF(2):

$$A = \begin{array}{ccccc} 1 & \zeta & \eta & \zeta\eta & \zeta\eta^2 \\ \left(\begin{matrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{matrix}\right. & \begin{matrix} 1\,0 \\ 0\,1 \\ 1\,1 \\ 1\,0 \\ 0\,1 \\ 1\,1 \\ 1\,0 \\ 0\,1 \\ 1\,1 \end{matrix} & \begin{matrix} 1\,0 \\ 1\,0 \\ 1\,0 \\ 0\,1 \\ 0\,1 \\ 0\,1 \\ 1\,1 \\ 1\,1 \\ 1\,1 \end{matrix} & \begin{matrix} 1\,0 \\ 0\,1 \\ 1\,1 \\ 0\,1 \\ 1\,1 \\ 1\,0 \\ 1\,1 \\ 1\,0 \\ 0\,1 \end{matrix} & \left.\begin{matrix} 1\,0 \\ 0\,1 \\ 1\,1 \\ 1\,1 \\ 1\,0 \\ 0\,1 \\ 0\,1 \\ 1\,1 \\ 1\,0 \end{matrix}\right) \end{array}$$

(4.2) says that the set $(\zeta, \zeta^2, \eta, \eta^2)$ has the P_2-property. Hence the set of classes (X_1^*, X_2^*) or simply (ζ, η) has the P_2-property over GF(2). Then the submatrix of A, formed by the four columns corresponding to ζ and η, has the P_2-property:

$$A_2 = \begin{pmatrix} 1&0&1&0 \\ 0&1&1&0 \\ 1&1&1&0 \\ 1&0&0&1 \\ 0&1&0&1 \\ 1&1&0&1 \\ 1&0&1&1 \\ 0&1&1&1 \\ 1&1&1&1 \end{pmatrix}$$

Finally (4.5) implies that $(1, \zeta, \zeta^2, \eta, \eta^2, \zeta\eta)$ has the P_5-property. Hence $(X_0^*, X_1^*, X_2^*, X_3^*)$ or simply $(1, \zeta, \eta, \zeta\eta)$ has the P_5-property over GF(2). It implies that the submatrix of A, formed by the first seven columns, has the P_5-property:

$$A_5 = \begin{pmatrix} 1&1&0&1&0&1&0 \\ 1&0&1&1&0&0&1 \\ 1&1&1&1&0&1&1 \\ 1&1&0&0&1&0&1 \\ 1&0&1&0&1&1&1 \\ 1&1&1&0&1&1&0 \\ 1&1&0&1&1&1&1 \\ 1&0&1&1&1&1&0 \\ 1&1&1&1&1&0&1 \end{pmatrix}$$

REFERENCES

[1] Bose, R. C. and Ray-Chaudhuri, D. K.,"On a class of error correcting binary group codes", Information and Control, vol. 3, No.1, March 1960, pages 68-79

[2] Bose, R. C. and Ray-Chaudhuri, D. K.,"Further results on error correcting binary group codes," Information and Control, vol. 3, No. 3, September 1960, pages 279-290.

[3] Bose, R. C., "On some connections between the design of experiments and information theory," To appear in Bulletin de l'Institut International de Statistique.

[4] Peterson, W. W., "Encoding and error correction procedures for Bose-Chaudhuri Codes," I.R.E. Trans. on Inform. Theory, September 1960.

[5] Van der Waerden, B. L., Modern Algebra, vol. 2, Frederick Ungar Pub. Co., New York.

[6] Zierler, Neal,"A class of cyclic, linear error-correcting codes in p^m symbols," M.I.T. Lincoln Laboratory Group report 55-19.

ACKNOWLEDGEMENT

I wish to express my deep gratitude to Professor R. C. Bose who taught me Coding Theory and its applications to Design of Experiments for suggesting the problem to me and for his guidance and encouragement throughout the preparation of this work.

INSTITUTE OF STATISTICS
NORTH CAROLINA STATE COLLEGE

(Mimeo Series available for distribution)

258. Hoeffding, Wassily. On sequences of sums of independent random vectors.
259. Webster, J. T., A. H. E. Grandage, R. J. Hader, R. L. Anderson. A decision procedure for the inclusion of an independent variate in a linear estimator. June, 1960.
260. Chakravarti, I. M. On some methods of construction of partially balanced arrays. July, 1960.
261. Roy, S. N. and R. Gnanadesikan. On certain alternative hypotheses on dispersion matrices. August, 1960.
262. Murthy, V. K. On the distribution of averages over the various lags of certain statistics related to the serial correlation coefficients. August, 1960.
263. Anderson, R. L. Some needed developments in multivariate analysis. August, 1960.
264. Chapman, D. G., W. S. Overton and A. L. Finkner. Methods of estimating dove kill. October, 1959.
265. Eicker, Friedhelm. Consistency of parameter-estimates in a linear time-series model. October, 1960.
266. Eicker, Friedhelm. A necessary and sufficient condition for consistency of the LS estimates in linear regression. October, 1960.
267. Smith, W. L. On some general renewal theorems for nonidentically distributed variables. October, 1960.
268. Duncan, D. B. Bayes rules for a common multiple comparisons problem and related Student-t problems. November, 1960.
269. Bose, R. C. Theorems in the additive theory of numbers. November, 1960.
270. Cooper, Dale and D. D. Mason. Available soil moisture as a stochastic process. December, 1960.
271. Eicker, Friedhelm. Central limit theorem and consistency in linear regression. December, 1960.
272. Rigney, Jackson A. The cooperative organization in wildlife statistics. Presented at the 14th Annual Meeting, Southeastern Association of Game and Fish Commissioners, Biloxi, Mississippi, October 23-26, 1960. Published in Mimeo Series, January, 1961.
273. Schutzenberger, M. T. On the definition of a certain class of automata. January, 1961.
274. Roy, S. N. and J. N. Shrizastaza. Inference on treatment effects and design of experiments in relation to such inferences. January, 1961.
275. Ray-Chaudhuri, D. K. An algorithm for a minimum cover of an abstract complex. February, 1961.
276. Lehman, E. H., Jr. and R. L. Anderson. Estimation of the scale parameter in the Weibull distribution using samples censored by time and by number of failures. March, 1961.
277. Hotelling, Harold. The behavior of some standard statistical tests under non-standard conditions. February, 1961.
278. Foata, Dominique. On the construction of Bose-Chaudhuri matrices with help of Abelian group characters. February, 1961.
279. Eicker, Friedhelm. Central limit theorem for sums over sets of random variables. February, 1961.
280. Bland, R. P. A minimum average risk solution for the problem of choosing the largest mean. March, 1961.
281. Williams, J. S., S. N. Roy and C. C. Cockerham. An evaluation of the worth of some selected indices. May, 1961.
282. Roy, S. N. and R. Gnanadesikan. Equality of two dispersion matrices against alternatives of intermediate specificity. April, 1961.
283. Schutzenberger, M. T. On the recurrence of patterns. April, 1961.
284. Bose, R. C. and I. M. Chakravarti. A coding problem arising in the transmission of numerical data. April, 1961.
285. Patel, M. S. Investigations on factorial designs. May, 1961.
286. Bishir, J. W. Two problems in the theory of stochastic branching processes. May, 1961.
287. Konsler, T. R. A quantitative analysis of the growth and regrowth of a forage crop. May, 1961.
288. Zaki, R. M. and R. L. Anderson. Applications of linear programming techniques to some problems of production planning over time. May, 1961.