AN APPLICATION OF INCOMPLETE BLOCK DESIGNS TO THE CONSTRUCTION OF ERROR-CORRECTING CODES

by

K. J. C. Smith
University of North Carolina

Institute of Statistics Mimeo Series No. 587

August, 1968

This research was supported by the National Science Foundation Grants No. GP-5790 and No. GU-2059 and by the Army Research Office, Durham, Grant No. DA-ARO-D-31-124-G910.

DEPARTMENT OF STATISTICS
UNIVERSITY OF NORTH CAROLINA
Chapel Hill, N. C.

1. Introduction

Historically, balanced and partially balanced incomplete block designs have been used primarily for statistical applications in the design of experiments. Recently, incomplete block designs have been used by several authors in constructing error-correcting codes. This approach has yielded useful and efficient constructions of codes.

This paper presents an application of incomplete block designs to the construction of error-correcting codes which may be decoded using a relatively simple majority logic decoding procedure. An identity matrix, I, is adjoined to the incidence matrix, N, of a balanced or partially balanced incomplete block design. The resulting matrix is taken as the parity check matrix of a linear code; a relatively simple majority logic decoding procedure for error correction may be used for the code.

A brief introduction to incomplete block designs and to linear codes is given in sections 2 and 3 for the reader unfamiliar with either area.

2. Incomplete Block Designs

2.1 Balanced Incomplete Block Designs

A balanced incomplete block (BIB) design is an arrangement of v objects, usually referred to as treatments, into b sets, called blocks, such that the following conditions are satisfied:

(i) each block contains k^*[1] distinct treatments;

(ii) each treatment occurs in r^*[1] distinct blocks;

(iii) each pair of treatments occur together in exactly λ different blocks.

The variables v, b, r^*, k^*, λ are referred to as the parameters of the design. The existence and construction of BIB designs are treated in detail by Bose (1939), Bose (1969), Hall (1967), and Ryser (1963), among others. Ryser (1963) uses the term (v,b,r^*,k^*,λ)- configuration for a BIB design with parameters v,b,r^*,k^*,λ.

The five parameters of a BIB design satisfy the following relations (see Bose (1969), for example):

(2.1.1) $\quad vr^* = bk^*,$

(2.1.2) $\quad \lambda(v-1) = r^*(k^*-1).$

Obviously, $\lambda \leq r^*$. If $0<\lambda<r^*$, then Fisher's inequality, Bose (1969), states that

(2.1.3) $\quad b \geq v.$

If b = v, then, from equation (2.1.1), $r^* = k^*$. In this case, the BIB design is said to be symmetrical.

---

[1] Traditionally, k and r are used as parameters of a design. We shall use k^* and r^* to avoid confusion with notation used in coding theory.

2.2 Partially Balanced Incomplete Block Designs

Before proceeding, we need the concept of an association scheme, Bose and Shimamoto (1952).

An m-class association scheme is a relation between v treatments satisfying the following conditions:

(a) any two treatments are either 1st, 2nd, ..., or m^{th} associates, the relation of association being symmetrical;

(b) each treatment has n_i i^{th} associates, the number n_i being independent of the treatment chosen.

(c) if α and β are i^{th} associates, then the number of treatments which are j^{th} associates of α and k^{th} associates of β is p_{jk}^{i} and is independent of the pari of i^{th} associates α and β. (i,j,k=1,2,...,m)

The parameters v, n_i, p_{jk}^{i} are not all independent. For example, $p_{jk}^{i} = p_{kj}^{i}$. Other relations among the parameters are given by Bose and Nair (1939).

Given an m-class association scheme of v treatments, a partially balanced incomplete block (PBIB) design is an arrangement of the v treatments into b blocks such that

(i) each block contains k* distinct treatments;

(ii) each treatment occurs in r* distinct treatments;

(iii) each pair of treatments which are i^{th} associates occur together in exactly λ_i blocks (i=1,2,...,m).

For a PBIB design based on an m-class association scheme with parameters v, n_i, p_{jk}^{i}, it is shown by Bose and Nair (1939), for example, that

(2.2.1) $$vr^* = bk^*$$

and

(2.2.2) $n_1\lambda_1+n_2\lambda_2+\ldots+n_m\lambda_m = r^*(k^*-1)$.

In general, the number of blocks need not be as large as the number of treatments.

A BIB design with parameters v,b,r^*,k^*,λ may be considered a PBIB design based on an association scheme with one class.

2.3 Incidence Matrix of a Design

Let us arbitrarily label and order the treatments of a PBIB (or BIB) design as

$$V_1, V_2, \ldots, V_v$$

and the blocks, similarily, as

$$B_1, B_2, \ldots, B_b.$$

We shall say that V_j is incident with B_i if the treatment V_j occurs in the block B_i. $(i=1,2,\ldots,b;\ j=1,2,\ldots,v.)$

The $b \times v$ incidence matrix, N, of the design is defined as the matrix

(2.3.1) $N = (n_{ij})_{b\times v}$

where

(2.3.2) $n_{ij} =$ 1, if V_j is incident with (occurs in) B_i;
0, otherwise. $(i=1,2,\ldots,b;\ j=1,2,\ldots,\ .)$

Clearly, each row of N contains k^* 1's and column of N contains r^* 1's.

3. Linear Error-Correcting Codes

3.1 Introduction

We state here a few basic concepts of linear error-correcting codes. The reader is referred to Peterson (1963) or to Berlekamp (1968) for further details. Only binary codes will be considered here.

A number of messages are to be transmitted over a noisy channel from a source to a destination. Each message corresponds to a sequence of n binary symbols, say 0 and 1, called a codeword. The n symbols of a codeword $\underline{t}'$[2] = $(t_1, t_2, \ldots, t_n)$ are transmitted consecutively over the channel. Random "noise" in the channel may cause a 0 to be received as a 1 or vice versa. If this happens, we shall say that a transmission error has occurred. The corresponding received sequence, $\underline{r}' = (r_1, r_2, \ldots, r_n)$ is not necessarily a codeword. Suppose $\underline{r}' = \underline{t}' + \underline{e}'$, where $\underline{e}' = (e_1, e_2, \ldots, e_n)$ is the unknown error vector; each coordinate of $\underline{e}'$ is a 0 or a 1 and the addition is in binary, i.e. over GF(2). The number of nonzero coordinates of $\underline{e}'$ is the number of errors which have occurred in transmitting $\underline{t}'$. We say that it is possible to correct s errors if, assuming at most s errors have occurred in transmitting a codeword, it is possible to determine correctly which coordinates of the corresponding error vector are nonzero. The correct transmitted codeword may then be obtained by complementing these coordinates of the received vector. This procedure is called decoding.

A binary linear (n,k) code C is a k-dimensional subspace of the n-dimensional vector space over GF(2). Each of the $2^k - 1$ nonzero vectors of C

---

[2] The notation $\underline{a}' = (a_1, a_2, \ldots, a_n)$ denotes a row vector; $\underline{a}$ denotes a column vector.

is a codeword; k is the number of information symbols of the code C. The redundancy of C is r = n-k.

A matrix whose rows span C is a generator matrix of the code. The orthogonal complement of C, in the usual algebraic sense, is the dual code C'. A parity check matrix of C is a matrix whose rows span the dual code C'. If H is a parity check matrix of C, then the vector $\underline{g}' = (g_1, g_2, \ldots, g_n)$ is a codeword of C if and only if

(3.1.1) $$H\underline{g} = \underline{0}$$

Each equation of (3.1.1), corresponding to the rows of H, is a parity check equation.

Suppose $\underline{t}'$ is a transmitted codeword and $\underline{r}'$ is the corresponding received vector. The error vector is $\underline{e}' = \underline{r}' - \underline{t}'$. Since $\underline{t}'$ is a codeword of C, then

$$H\underline{t} = \underline{0}$$

and

(3.1.2) $$H\underline{r} = H\underline{t} + H\underline{e} = H\underline{e} = \underline{s}, \text{ say .}$$

The vector $\underline{s} = H\underline{r}$ is called the symdrome of the received vector $\underline{r}'$. Equation (3.1.2) may be used for decoding. The syndrome of a received word is calculated and the equation

$$H\underline{e} = \underline{s}$$

may be solved, in some instances, for the unknown error vector $\underline{e}'$, assuming at most m, say, of the coordinates of $\underline{e}'$ are nonzero.

3.2 Systematic codes

If G is the generator matrix of a linear code C and G* is obtained from G by column permutations, then G* generates a linear code C* defined to be equivalent to C. Given a (n,k) linear code C, we can find an equivalent code C* for which the generating matrix is

$$G = [I_k, P]$$

where I_k is the k x k identity matrix and P is a k x (n-k) matrix. Every codeword of C* is a linear combination of the rows of G* and is of the form

$$(c_1, c_2, \ldots, c_k, c_1p_{11}+c_2p_{21}+\ldots+c_kp_{k1}, \ldots, c_1p_{1r}+c_2p_{2r}\ldots+c_kp_{kr}),$$

where $c_1, c_2, \ldots, c_k$ are arbitrary and $P = (p_{ij})_{kxr}$, $r = n-k$. Thus the first k coordinates of a codeword of C* may be arbitrarily chosen. The remaining coordinates are linear combinations of these coordinates. The first k coordinates are information places and the remaining r coordinates are redundant places. Such a code is called a systematic code.

We shall now consider a systematic (n,k) code C with generator matrix

$$G = [I_k, P]$$

for some P. Let

$$H = [P^T, I_r],$$

where P^T denotes the transpose of P. Over GF(2),

$$HG^T = [P^T \; I_r] \begin{bmatrix} I_k \\ P^T \end{bmatrix}$$

$$= P^T + P^T$$

$$= 0$$

Thus the vector space generated by the rows of H is orthogonal to that generated by G, i.e., H is a parity check matrix for C.

Since the first k coordinates of a codeword in a systematic code completely specify the codeword, only these symbols in a received vector need be decoded. The remaining r redundant symbols may be determined from the first k symbols to form the decoded codeword if necessary.

3.3 Majority-logic decoding

The technique of majority-logic decoding of linear codes was developed by Massey (1963) for particular linear codes. This procedure is based on the concept of a set of parity check equations orthogonal on a given symbol.

Let C be an (n,k) linear code and suppose it is possible to find a set of J vectors of the dual code C', say

(3.3.1) $\underline{h}'_j = (h_{j1}, h_{j2}, \ldots, h_{jn})$, $j = 1,2,\ldots,J$

such that for fixed m, m = 1,...,n

$h_{jm} = 1$ for each $j = 1,2,\ldots,J$

(3.3.2) $h_{ju} = 0$ for all but at most one $j = 1,2,\ldots,J$ and for any fixed $u \neq m$.

That is, each of the J vectors $\underline{h}'_j$ has m^{th} coordinate 1 and at most one of these J vectors has u^{th} coordinate 1 for any $u \neq m$. Then the set of J equations

(3.3.3) $h_{j1}e_1 + h_{j2}e_2 + \ldots + h_{j,n}e_n = s_j$, $u=1,2,\ldots,J$

are said to be orthogonal on the symbol e_m. (Massey (1963)). If the set of equations (3.3.3) corresponds to a set of parity check equations for a linear code C, then a majority-logic procedure may be used to determine the error symbol e_m and thus decode the received symbol r_m into the corresponding symbol t_m from the following theorem.

Theorem 3.3.1 Suppose a set of J parity check equations (3.3.3) orthogonal as the symbol e_m may be found for a linear code C. Then, provided at most $\left[J/2\right]$[3] errors have occured, the symbol e_m is given correctly by the following rule:

---

[3] The notation [x] denotes the greatest integer less than or equal to x.

(1) e_m is that value of GF(2) which is assumed by the majority (greatest fraction) of the $\{s_j\}$, provided such a value exists;

(2) e_m is zero if the $\{s_j\}$ take on the values 0 and 1 with equal frequency.

This theorem is proved by Massey (1963). We shall omit the proof here and prove a generalization of the theorem which does not assume the orthogonality of the parity check equations on a particular symbol. This generalization appears in Rudolph (1967) and Smith (1967).

Theorem 3.3.2 Let C be a linear (n,h) code and let

$$h_{j1}e_1+h_{j2}e_2+\ldots+h_{jn}e_n = s_j \quad , \; j = 1,2,\ldots,J \tag{3.3.4}$$

be a set of J parity check equations such that

$$h_{jm} = 1 \quad , \; j = 1,2,\ldots,J. \tag{3.3.5}$$

Assume that for any $u \neq m$,

$$h_{ju} = 1 \text{ for at most } \lambda \text{ subscripts } j = 1,2,\ldots,J. \tag{3.3.6}$$

Then, provided at most $\left[J/2\lambda\right]$ errors have occurred, the symbol e_m is given correctly by the following rule:

(1) e_m is that value of GF(2) which is assumed by the greatest fraction of the $\{s_j\}$, if such a most frequent value exists.

(2) e_m is zero if the $\{s_j\}$ take on the values 0 and 1 with equal frequency.

Proof: Suppose at most $t = \left[J/2\lambda\right]$ errors have occurred. Then at most t of the symbols $e_1, e_2, \ldots, e_n$ are nonzero. If all symbols other than e_m were zero, then

$$s_j = e_m \quad , \; j = 1,2,\ldots,J \tag{3.3.7}$$

and the decision rule of the theorem is correct. If one of the other symbols is nonzero, then at most λ of the s_j in equation (3.3.7) are different from e_m. In general, if x other symbols are nonzero, at most $x\lambda$ of the s_j in equation (3.3.7) are different from e_m, since each of these symbols can

affect at most λ of the s_j.

If $e_m = 0$, then if t or fewer of the error symbols are nonzero, at most $t\lambda$ of the s_j are nonzero. Since $J \geq 2t\lambda$, then the decision rule of the theorem gives the correct value of e_m.

If $e_m = 1$, then if (t-1) or fewer of the other error symbols are nonzero, at most $(t-1)\lambda$ of the s_j are different from e_m. Since $J > 2(t-1)\lambda$, then the greatest fraction of the s_j are equal to 1 and the decision rule of the theorem gives the correct value of e_m.

3.4 Majority Decodable Codes

A number of linear codes have been shown to be decodable using majority logic techniques. Among these are the Reed-Muller codes and their generalizations discussed by Kasami et al (1968) and Weldon (1968), as well as the codes termed "geometric codes" by Goethals and Delsarte (1967), Rudolph (1967) and Smith (1967). Townsend and Weldon (1967) have investigated a class of codes called quasi-cyclic self-orthogonal codes, to which a majority logic decoding algorithm may be applied. With the exception of the latter codes and some special cases of the other codes mentioned above, the problem of determining a general expression for the number of information symbols in these codes is difficult and has not yet been completely solved.

To avoid this difficulty, we shall present in section 4 a class of linear codes which may be majority logic decodable and for which the number of information symbols is immediately determined. Special cases of these codes are equivalent to the quasi-cyclic self orthogonal codes discussed by Townsend and Weldon (1967).

4. Systematic Block Design Codes

4.1 Definition

We define a large class of linear codes, which we shall call systematic block design codes, as follows.

Let N be the b x v incidence matrix, defined in section 2.3, of a balanced or partially balanced incomplete block design D with parameters $v,b,r^*,k^*,\lambda_1,\ldots,\lambda_m$. Let I_b be an identity matrix of order b. The systematic block design code (associated with the design D) is the (binary) linear code orthogonal to the row space of the matrix

(4.1.1) $$H = [N, I_b],$$

that is, the linear code for which H is a parity check matrix.

The systematic block design code associated with the matrix H has the following immediate properties.

(1) The length of the code is n = v+b

(2) The redundancy is r = b.

(3) The number of information symbols is k = n-r=v.

(4) The code is systematic but not necessarily cyclic.

(5) The generator matrix of the code is

(4.1.2) $$G = [I_v, N^T]$$

(6) The information rate $R \equiv k/n$ is

(4.1.3) $$R = \frac{v}{v+b} = \frac{1}{1+b/v} .$$

Clearly, $R \leq \frac{1}{2}$ if and only if $b \geq v$. For a BIB design $b \geq v$. Thus we may state

Lemma 4.1.1 The information rate of a systematic block design code associated with a BIB design is at most $\frac{1}{2}$.

In searching for a high rate ($R > \frac{1}{2}$, say) systematic block design code, we

must therefore restrict our attention to codes associated with PBIB designs for which $b<v$. Some examples of such codes will be given in section 4.4.

4.2 Encoding and Decoding

Since the codes are systematic, the encoding or construction of codewords is relatively simple. The first $k = v$ symbols may be chosen arbitrarily; the remaining $r = b$ redundant symbols are linear combinations, determined by the generator matrix in equation (4.1.2), of the k information symbols.

A relatively simple majority logic decoding procedure may be used for the systematic block design codes. We state this as a theorem.

Theorem 4.2.1. Let C be a systematic block design code associated with a (partially) balanced incomplete block design D with parameters $v,b,r^*,k^*,$ $\lambda_1,\ldots,\lambda_m$. Let

$$\lambda = \max_{1\le i\le m} \lambda_i \tag{4.2.1}$$

Up to $\left\lceil r^*/2\lambda \right\rceil$ errors may be corrected using a one-step majority logic decoding procedure.

Proof: It is necessary to correct only the information symbols, for the redundant symbols may then be determined from the encoding procedure. Each row of the parity check matrix of the code determines a parity check equation. If N is the incidence matrix of the associated design, then the parity check matrix for the code is

$$H = [N, I].$$

Each of the first $k = v$ information symbols corresponds to a treatment in the design. Each row of H corresponds to a block. The first k entries in a row are 1 or 0, according to whether the appropriate treatment occurs or does not occur in the corresponding block. Each treatment occurs in r^* blocks.

Consider any one of the v treatments, say V_a and the r* rows of H corresponding to the blocks in which V_a occurs. Each of the r* parity check equations determined by these rows, say

$$h_{j1}e_1 + h_{j2}e_2 + \ldots + h_{jn}e_n = s_j. \tag{4.2.2}$$

Let us relabel the rows such that these are the first r* rows of H. Then for $j = 1,2,\ldots,r^*$,

$$h_{ja} = 1.$$

If treatment V_u and V_a are i^{th} associates, then

$$h_{ju} = 1 \text{ for at most } \lambda_i \text{ subscripts } j = 1,2,\ldots,r^* \text{ and for any fixed } u \neq a,\ 1 \leq u \leq v.$$

Moreover,

$$h_{ja} = 1 \text{ for at most one } j = 1,2,\ldots,r^* \text{ if } v+1 \leq a \leq n.$$

Thus, if $\lambda = \max_{1 \leq i \leq m} \lambda_i$, then

$$h_{ja} = 1 \text{ for } j = 1,2,\ldots,r^*$$
$$h_{ju} = 1 \text{ for at most } \lambda \text{ subscripts } j = 1,2,\ldots,r^* \text{ and for any fixed } u \neq a. \tag{4.2.3}$$

Hence, from Theorem 3.3.2, a majority logic decoding procedure may be used to determine e_a. This will give e_a correctly if at most $\left[r^*/2\lambda\right]$ errors have occurred. The procedure is to consider the set of r* parity check equations corresponding to the blocks in which treatment V_a occurs. The symbol e_a is given as that value of GF(2) which is assumed by the greatest fraction of the corresponding s_j in the syndrome vector. If no such greatest fraction exists, then e_a is zero.

This procedure is repeated for each of the remaining v-1 information symbols and yields the information symbols of the codeword corresponding to a received word correctly, provided at most $\left[\frac{r}{2\lambda}\right]$ errors have occurred.

4.3 Systematic Block Design Codes Associated With BIB Designs

A systematic block design code associated with a BIB design with parameters v,b,r^*,k^*,λ is a (n,k) linear code with $n = v+b$ and $k = v$. The majority-logic decoding procedure described in section 4.2 will correct up to $\left[r^*/2\lambda\right]$ errors. In this section, we give a few examples of these codes associated with particular BIB designs.

The literature on BIB designs is extensive and includes many constructions for a wide range of design parameters. The reader is referred to Bose (1969) for a comprehensive treatment of such designs and to methods of constructing the designs mentioned below.

BIB designswith $k^* = 3$ and $\lambda = 1$ are called Steiner triple systems. It may be shown that these conditions imply that r^* must be of the form $3t+1$ or $3t$ for some positive integer t. In the case $r^* = 3t+1$, the parameters are

$$v = 6t+3,\ b = (3t+1)(2t+1),\ r^* = 3t+1,\ k^* = 3,\ \lambda = 1.$$

This series of designs is referred to as the T_1 series and exists for all values of t. The systematic block codes associated with the T_1 designs have

$$n = v+b = (2t+1)(3t+4)$$

$$k = v = 6t+3$$

$$R = k/n = \frac{3}{3t+4}$$

and the majority decoding procedure described earlier will correct up to $\left[r^*/2\lambda\right] = \left[\frac{3t+1}{2}\right]$ errors. Table 4.3.1 lists these parameters of the codes with some of the T_1 series of designs.

TABLE 4.3.1

Systematic Block Design Codes Associated With T_1 Series

$v = 6t+3,\ b = (3t+1)(2t+1),\ r^* = 3t+1,\ k^* = 3,\ \lambda = 1$

t	Code Length	Information Symbols	Rate	Errors Corrected
1	21	9	.43	2
2	50	15	.30	3
3	91	21	.23	5
4	144	27	.19	6
5	209	33	.16	8
6	286	39	.13	9

These codes have low rates and only a relatively small number of errors are guaranteed correctable by the majority decoding procedure.

A different series of BIB designs with $\lambda = 1$ are the BIB designs constructed from finite projective planes. These designs are often called the orthogonal series 2 or OS2 series. The parameters are

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

Such designs are known to exist when s is a prime power. The associated systematic block design codes have

$$n = v+b = 2(s^2+s+1),$$

$$k = v = 2(s^2+s+1),$$

$$R = k/n = \tfrac{1}{2},$$

and up to $\left[r^*/2\lambda\right] = \left[\frac{s+1}{2}\right]$ errors may be corrected by our decoding procedure. These parameters of some codes are exhibited in Table 4.3.2.

TABLE 4.3.2

Systematic Block Design Codes Associated With OS2 Series

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

s	Code Length	Information Symbols	Rate	Errors Corrected
2	14	7	.5	1
3	26	13	.5	2
4	42	21	.5	2
5	62	31	.5	3
7	114	57	.5	4
8	146	73	.5	4

While these codes have rate .5, the number of errors corrected is still relatively small.

4.4 Systematic Block Design Codes Associated with PBIB Designs

A systematic block design code associated with a PBIB design with parameters $v,b,r^*,k^*,\lambda_1,\ldots,\lambda_m$ has $n = v+b$ and $k = v$. If $\lambda = \max_{1\le i\le m} \lambda_i$, then up to $\left[r^*/2\lambda\right]$ errors may be corrected using the majority-logic decoding procedure described in Section 4.2.

Of particular interest are the PBIB designs with $b<v$, for the rates of the associated codes are greater than $\frac{1}{2}$. We shall consider here codes associated with some PBIB designs based on partial geometries, Bose (1963), for which $b<v$.

If the roles of treatments and blocks of a BIB design with $\lambda = 1$ are interchanged, then the resulting design, called the dual design, is a PBIB

design with parameters b,v,k*,r*,1,0. This notation implies that the number of treatments is b, etc.

Consider the T_1 series of BIB designs, discussed in section 4.3. The dual designs are PBIB designs with parameters

$$v = (3t+1)(2t+1),\ b = 6t+3,\ r^* = 3,\ k^* = 3t+1,\ \lambda_1 = 1,\ \lambda_2 = 0.$$

The resulting systematic block design codes have

$$n = (2t+1)(3t+4)$$

$$k = (3t+1)(2t+1)$$

$$R = \frac{3t+1}{3t+4}$$

and the majority decoding procedure will correct up to $\left[3/2\right] = 1$ error. Table 4.4.1 exhibits these properties of some such codes.

TABLE 4.4.1

Systematic Block Design Codes Associated With Duals of T_1 Designs

$v = (3t+1)(2t+1),\ b = 6t+1,\ r^* = 3,\ k^* = 3t+1,\ \lambda_1 = 1,\ \lambda_2 = 0$

t	Code Length	Information Symbols	Rate	Errors Corrected
1	21	12	.57	1
2	50	35	.70	1
3	91	70	.77	1
4	144	117	.81	1
5	209	176	.84	1
6	286	247	.86	1

These codes have high rates, although only a single error is guaranteed correctable by the majority decoding procedure. The latter property is not necessarily a disadvantage, however.

A more interesting PBIB design is that obtained from the configuration of points and generators on an elliptic non-degenerate quadric Q_5 in the finite projective space PG(5,s). Taking treatments as generators and blocks as points, we obtain a PBIB design with parameters.

$$v = (s^2+1)(s^3+1),\ b = (s+1)(s^3+1)\ ,\ r^* = s+1,\ k^* = s^2+1,\ \lambda_1 = 1,\ \lambda_2 = 0.$$

This design is discussed by Ray-Chaudhuri (1962) and Bose (1963). Table 4.4.2 gives the parameters of the associated symmetric block design code for a few values of s, s being a prime power.

TABLE 4.4.2

Systematic Block Design Codes Associated With The PBIB Design

$v = (s^2+1)(s^3+1),\ b = (s+1)(s^3+1),\ r^* = s+1,\ k^* = s^2+1,\ \lambda_1 = 1,\ \lambda_2 = 0$

s	Code Length	Information Symbols	Rate	Errors Corrected
2	72	45	.63	1
3	392	280	.71	2
4	1430	1105	.77	2
5	4032	3276	.81	3

4.5 Discussion

A systematic block design code associated with an incomplete block design with v treatments and b blocks has rate $R = \frac{v}{v+b}$. If $b \geq v$, then $R < \frac{1}{2}$.

If the associated design is a (P)BIB design with parameters $v, b, r^*, k^*, \lambda_1, \ldots, \lambda_m$, then, from equation (2.1.1),

$$b = \frac{vr^*}{k^*}$$

and

$$R = \frac{k^*}{k^*+r^*} = \frac{1}{1+r^*/k^*}$$

Since the more interesting codes are those whose rates are bounded away from zero, designs for which r^*/k^* is bounded will be more useful.

The number of errors corrected by the majority logic decoding procedure is $\left[r^*/2\lambda\right]$. Thus, designs with relatively large values of r* and relatively small values of $\lambda = \max_{1\leq i\leq m} \lambda_i$ will also be of interest.

Designs with r* relatively large have not yet been investigated as thoroughly as those with $r^* \leq 20$, Until the advent of computers, designs with large values of r* and k* have been impractical for statistical application. However, further research on these designs may yield important results in such areas as the constructions of error-correcting codes.

The number of errors guaranteed correctable by a majority decoding procedure of the systematic block design codes is relatively small. However, a more important property of a code is the average probability of incorrect decoding. An upper bound on the probability of a decoding error may be calculated for the systematic block design codes for which $\lambda = 1$. This will be the subject of a separate report.

REFERENCES

1. Berlekamp, E. R. (1968). Algebraic Coding Theory, McGraw-Hill, New York.

2. Bose, R. C. (1939). "On the construction of balanced incomplete block designs," Ann. Eugenics, 9, 353-399.

3. Bose, R. C. (1963). "Strongly regular graphs, partial geometries and partially balanced designs," Pac. J. Math., 13, 389-419.

4. Bose, R. C. (1969). Combinatorial Problems of Experimental Designs, Vol I, John Wiley and Sons, New York, (to appear).

5. Bose, R. C. and Nair, K. R. (1939). "Partially balanced incomplete block designs," Sankhya, 4, 337-372.

6. Bose, R. C. and Shimamoto, T. (1952). "Classification and analysis of partially balanced designs with two associate classes," J. Amer. Statist. Assoc., 47, 151-184.

7. Goethals, J. M. and Delsarte, P. (196). "On a class of majority logic decodable cyclic codes," IEEE Trans. on Information Theory, IT-14, 182-188.

8. Hall, M., Jr. (1967). Combinatorial Theory, Blaisdell, Wathham, Mass.

9. Kasami, T., S. Lin and W. W. Peterson. (1968). "New generalizations of the Reed-Muller codes - Part I: Primitive codes," IEEE Trans. on Information Theory, It-14, 189-198.

10. Massey, J. L. (1963). Threshold Decoding, M.I.T. Press, Cambridge, Mass.

11. Peterson, W. W. (1961). Error-Correcting Codes, M.I.T. Press, Cambridge, Mass.

12. Ray-Chaudhuri, D. K. (1962). "Application of the geometry of quadrics for constructing PBIB designs," Ann. Math. Statist., 33, 1175-1186.

13. Rudolph, L. D. (1967). "A class of majority logic decodable codes," IEEE Trans. on Information Theory, IT-13, 305-307.

14. Ryser, H. J. (1963). Combinatorial Mathematics, Carus Math. Monograph No. 14, Mathematical Association of America, Buffalo, N. Y.

15. Smith, K. J. C. (1967). "Majority decodable derived from finite geometries," Institute of Statistics Mimeo Series No. 561, Department of Statistics, University of North Carolina.

16. Townsend, R. L. and Weldon, E. J., Jr. (1967). "Self-orthogonal quasi-cyclic codes," IEEE Trans. on Information Theory, IT-13, 183-194.

17. Weldon, E. J., Jr. (1968). "New generalizations of the Reed-Muller codes - Part II: Nonprimitive codes." IEEE Trans. on Information Theory, IT-14, 199-205.