INFORMATION AND CONTROL 3, 279–290 (1960)

Further Results on Error Correcting Binary Group Codes*

R. C. BOSE AND D. K. RAY-CHAUDHURI

University of North Carolina and Case Institute of Technology

The present paper is a sequel to the paper "On a class of error-correcting binary group codes", by R. C. Base and D. K. Ray-Chaudhuri, appearing in *Information and Control* in which an explicit method of constructing a t-error correcting binary group code with $n = 2^m - 1$ places and $k = 2^m - 1 - R(m,t) \geqq 2^m - 1 - mt$ information places is given. The present paper generalizes the methods of the earlier paper and gives a method of constructing a t-error correcting code with n places for any arbitrary n and $k = n - R(m,t) \geqq [(2^m - 1)/c] - mt$ information places where m is the least integer such that $cn = 2^m - 1$ for some integer c. A second method of constructing t-error correcting codes for n places when n is not of the form $2^m - 1$ is also given.

SECTION I

This paper is a continuation of our previous paper, Bose and Ray-Chaudhuri (1960), "On a class of error correcting binary group codes." The notation used there will be followed throughout, with the minimum of explanation.

It was shown that we can obtain a t-error correcting n-place binary group code (n,k) with k information places, if $n = 2^m - 1$ and $k = n - R(m,t)$ where $R(m,t) \leqq mt$ is the rank of a certain matrix whose properties have been investigated. Peterson (1960) has investigated certain interesting properties of these codes, and given the exact value of $R(m,t)$. In Section II, we have generalized our results to the case when $n = (2^m - 1)/c$ where c is the smallest integer for which $cn + 1$ is a power of 2. This generalization enables us to obtain as a special case certain

* 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.

codes with the same values of n and k as those investigated by Prange (1958–1959).

Let V_r denote the vector space of r-vectors with coordinates from $GF(2)$. Following the notation of Bose and Chaudhuri (1960) we shall denote by $n_{2t}(r)$ the maximum number of vectors that it is possible to choose in V_r such that no $2t$ are dependent. A matrix with elements from $GF(2)$ is said to possess the property (P_{2t}) if no set of $2t$ rows are dependent. It was shown in our earlier paper that the problem of finding a t-error correcting n-place binary group code (n,k) with k information places, and the maximum transmission rate k/n can be completely solved if we can determine $n_{2t}(r)$ for every value of r and can construct a matrix with r columns and $n_{2t}(r)$ rows, possessing the property (P_{2t}). We constructed a matrix with mt columns and $2^m - 1$ rows, possessing the property (P_{2t}), which establishes the inequality

$$n_{2t}(mt) \geqq 2^m - 1 \tag{1}$$

In Section III, of the present paper we shall find lower bounds for $n_{2t}(r)$ for values of r which are not multiples of t, and construct the corresponding matrix with the property (P_{2t}). This enables us in certain instances to obtain t-error correcting (n,k) binary group codes for which the transmission rate k/n is better than for codes obtainable by using corollary 1, Theorem 1 of our earlier paper.

In Section IV we have given a table which, for given $n \leqq 100$ and $t \leqq 6$, enables us to calculate the best corresponding value of k obtainable by our methods.

SECTION II

For a given positive integer n, let $c = c(n)$ be the smallest integer such that $1 + cn$ is a power of 2. Let this power be denoted by $m = m(n)$. Thus,

$$n = (2^m - 1)/c \tag{2}$$

For example, if $n = 21$, then $c = 3$, $m = 6$; if $n = 31$, $c = 1$, $m = 5$. Again, if $n = 73$, $c = 7$, $m = 9$.

Let x be a primitive element of the Galois field $GF(2^m)$. Then

$$1, x, x^2, \cdots, x^{nc-1}$$

are all the distinct nonzero elements of the field and

$$x^{nc} = 1.$$

Each element of $GF(2^m)$ can be expressed as a polynomial of degree $m-1$ or less with coefficients from $GF(2)$. Let V_m be the vector-space of m-vectors, with elements from $GF(2)$. Then, as explained in Bose and Ray-Chaudhuri (1960) we can institute a (1,1) correspondence between the vector $\alpha = (a_0, a_1, \cdots, a_{m-1})$ of V_m, and the element

$$a_0 + a_1 x + \cdots + a_{m-1} x^{m-1}$$

of $GF(2^m)$. Then the null vector α_0 of V_m corresponds to the null element of $GF(2^m)$, and the sum of any two vectors of V_m corresponds to the sum of the corresponding elements of $GF(2^m)$. We can then identify the vector α of V_m and the corresponding element of $GF(2^m)$. This in effect defines a multiplication of the vectors of V_m and converts it into a field. In particular, we can speak of the powers of any vector. Let us set

$$\begin{aligned} \alpha_i = x^{ci} &= a_{i0} + a_{i1} x + \cdots + a_{i,m-1} x^{m-1} \\ &= (a_{i0}, a_{i1}, \cdots, a_{i,m-1}) \end{aligned} \tag{3}$$

where $i = 1, 2, \cdots, n$. Then $\alpha_1, \alpha_2, \cdots, \alpha_n$ are all the distinct elements of $GF(2^m)$ which are powers of x^c, that is, α_1. In particular, $\alpha_n = x^{cn} = 1$. Let

$$\alpha_i^* = (\alpha_i, \alpha_i^3, \cdots, \alpha_i^{2t-1}) \tag{4}$$

and

$$M^* = \begin{Vmatrix} \alpha_1, & \alpha_1^3, & \cdots & \alpha_1^{2t-1} \\ \alpha_2, & \alpha_2^3, & \cdots & \alpha_2^{2t-1} \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_n, & \alpha_n^3, & \cdots & \alpha_n^{2t-1} \end{Vmatrix} \tag{5}$$

When the α_i's are regarded as m-vectors over $GF(2)$, M^* is a matrix of order $n \times mt$ with elements from $GF(2)$. We shall now prove

LEMMA 1. Any $2t$ row vectors belonging to M^* are independent, i.e., M^* possesses the property (P_{2t}).

This result was proved in our earlier paper by using the properties of power sums. It is possible to generalize this proof. However, we shall give the following alternative proof based on considerations suggested by W. W. Peterson in a private communication.

Let $\beta_1, \beta_2, \cdots, \beta_{2t}$ be any $2t$ elements of $GF(2^m)$ chosen out of $\alpha_1, \alpha_2, \cdots, \alpha_n$. We then have to show that the matrix

$$D = \begin{Vmatrix} \beta_1 & \beta_1^3 & \cdots & \beta_1^{2t-1} \\ \beta_2 & \beta_2^3 & \cdots & \beta_2^{2t-1} \\ \vdots & \vdots & & \vdots \\ \beta_{2t} & \beta_{2t}^3 & \cdots & \beta_{2t}^{2t-1} \end{Vmatrix}$$

has rank $2t$. Since $x \to x^2$ is an automorphism of $GF(2^m)$, any linear relation between $\beta_1^u, \beta_2^u, \cdots, \beta_{2t}^u$ implies a corresponding linear relation among $\beta_1^{2u}, \beta_2^{2u}, \cdots, \beta_{2t}^{2u}$ and vice versa. Hence, the rank of

$$D_1 = \begin{Vmatrix} \beta_1 & \beta_1^2 & \cdots & \beta_1^{2t-1} & \beta_1^{2t} \\ \beta_2 & \beta_2^2 & \cdots & \beta_2^{2t-1} & \beta_2^{2t} \\ \vdots & \vdots & & \vdots & \vdots \\ \beta_{2t} & \beta_{2t}^2 & \cdots & \beta_{2t}^{2t-1} & \beta_{2t}^{2t} \end{Vmatrix}$$

is the same as the rank of D. However.

$$\det D_1 = \beta_1\beta_2 \cdots \beta_{2t} \prod_{j<i}^{2t} (\beta_i - \beta_j) \neq 0$$

since $\beta_1, \beta_2, \cdots, \beta_{2t}$ are all distinct and nonzero. This shows that rank $(D_1) = 2t$ and completes the proof of the Lemma.

Let $mt < n$. The columns of M^* are not always independent as is clear from the example for the case $n = 15$, $c = 1$, $m = 4$, $t = 3$, discussed in Section 5 of Bose and Chaudhuri (1960). As before, we shall denote the rank of M^* by $R(m,t)$. If $R(m,t) < mt$, then we can choose $R(m,t)$ independent columns of M^* and drop the remaining columns of M^* and thus get a matrix of order $n \times R(m,t)$ with the property (P_{2t}).

LEMMA 2. The rank $R(m,t)$ is the number of distinct residue classes (mod n) among the integers $2^j u (u = 1, 3, \cdots, 2t - 1; j \geqq 0)$.

This Lemma has been proved by Peterson (1960) for the special case $c = 1$, and his proof can be easily extended to the general case. We shall make a few remarks useful for application of the Lemma.

Denote by $(2^j u)$ the residue class corresponding to the integer $2^j u$. Since

$$\begin{aligned} 2^m u &= (2^m - 1)u + u \\ &= ncu + u \\ &= u (\text{mod } n) \end{aligned}$$

there cannot be more than m distinct residue classes among $(2^j u)$ with a fixed value of u, and in counting the number of residue classes it is suffi-

cient to confine ourselves to values of j in the range $0 \leqq j \leqq m - 1$. Hence,

$$R(m,t) \leqq mt.$$

If we arrange the integers $2^j u$ reduced (mod n) in a rectangular scheme, each row corresponding to one value of u, then

(i) If k is the least nonzero positive integer such that

$$u = 2^k u (\text{mod } n)$$

then $k \leqq m$. If $k = m$ the residue classes in the corresponding row are all distinct. If $k < m$, then k is a factor of m, and there are k distinct residue classes in the corresponding row.

(ii) If any two rows have one element in common they coincide entirely.

(a) To u we can associate the set of m columns of the submatrix

$$M_u^* = \begin{Vmatrix} \alpha_u \\ \alpha_u^3 \\ \vdots \\ \alpha_u^n \end{Vmatrix} \tag{6}$$

of M. The number of independent columns in M_u^* is exactly k. We can therefore delete $m - k$ suitable columns from M_u^* without changing the rank of M^*, or the property (P_{2t}).

(b) When two rows of the scheme corresponding to say u_1 and $u_2 (u_1 < u_2 \leqq 2t - 1)$ are identical we can delete the submatrix $M_{u_2}^*$ without changing the rank of M^* or the property (P_{2t}).

After the operations (a) and (b) we get from M^* a matrix of order $n \times R(m,t)$ with rank $R(m,t)$ and possessing the property (P_{2t}). Let the matrix so obtained be called A^* which is of order $n \times R(m,t)$ and possesses the property (P_{2t}).

The matrix A^* can serve as the parity check matrix.

Using Theorem 1 of Bose and Chaudhuri (1960) we now get the following results:

THEOREM 1. If n is any integer, and c is the least integer such that $1 + cn = 2^m$, then there exists a t-error correcting binary group code (n,k) for which the number of information places is

$$k = n - R(m,t)$$

where $R(m,t)$ is given by Lemma 2. The letters of the code are binary

n-vectors orthogonal to the columns of A^*, i.e., form the left null-space of A^*, where A^* is the matrix defined in the remarks following Lemma 2.

Every n-place binary sequence $(a_0, a_1, \cdots, a_{n-1})$ may be regarded as a polynomial $a_0 + a_1 y + \cdots + a_{n-1}y^{n-1}$ in an indeterminate y. Let R_n denote the set of all such polynomials of degree less than n with coefficients 0 and 1. The addition of polynomials in R_n can be defined in the usual way, i.e., by adding the coefficients mod 2. Let the multiplication be defined mod 2 and mod $(y^n - 1)$. With these operations R_n becomes a ring. Let

$$A^* = \begin{Vmatrix} b_{10} & b_{20} & \cdots & b_{r0} \\ b_{11} & b_{22} & \cdots & b_{r1} \\ \vdots & & & \\ b_{1,n-1} & b_{2,n-1} & \cdots & b_{r,n-1} \end{Vmatrix}$$

and let

$$\beta_i' = (b_{i0}, b_{i1}, \cdots, b_{i,n-1}), \qquad i = 1, 2, \cdots, r = R(m,t)$$

Let $\bar{V}(A^*)$ denote the vector space generated by $\beta_1', \beta_2', \cdots, \beta_r'$, and $V(A^*)$ denote the vector space orthogonal to $\bar{V}(A^*)$. If now the vectors of $V(A^*)$ are regarded as polynomials, then for the case $c = 1$, Peterson (1960) has proved that $V(A^*)$ is an ideal in R_n, generated by a certain polynomial $f(y)$ of degree $r = R(m,t)$. Peterson's arguments at once extend to the general case and we have the following:

Let $f_j(x)$ be the minimum polynomial of x^{cj} over $GF(2)$, where x is a primitive element of $GF(2^m)$. Then $V(A^*)$ is the ideal generated by

$$f(y) = \underset{j=1,3,\cdots,(2t-1)}{L.C.M.} f_j(y)$$

The polynomial $f(y)$ can also be expressed in an alternative form. Let $(p_1, p_2, \cdots, p_r)$ be a set of $r = R(m,t)$ integers containing one integer for each of the $R(m,t)$ distinct residue classes considered in Lemma 2. Then

$$f(y) = (y - x^{cp_1})(y - x^{cp_2}) \cdots (y - x^{cp_r}).$$

For a polynomial $f(y) = a_0 + a_1 y + \cdots a_{n-1}y^{n-1}$ we shall call $(a_{n-1}, a_{n-2}, \cdots, a_0)$ the reversed vector corresponding to $f(y)$. Let

$$\bar{f}(y) = (y^n - 1)/f(y)$$

and let $I[\bar{f}(y)]$ denote the set of 2^r reversed vectors corresponding to the

2^r polynomials of the ideal generated by $\bar{f}(y)$. Peterson's arguments then show that

$$\bar{V}(A^*) = I[\bar{f}(y)]$$

It follows that we can take

$$A^* = [\beta_1, \beta_2, \cdots, \beta_r]$$

where β_i' is the reversed vector corresponding to the polynomial

$$y^{i-1}\bar{f}(y), \qquad (i = 1, 2, \cdots, r),$$

and β_i is the transpose β_i'.

Example 1. Let $n = 21$. Then $c = 3$, $m = 6$. Let $t = 2$. To determine $R(m,t)$, we write the integers $2^j u (u = 1, 3; j = 0,1,2,3,4,5)$ in the following scheme, each row corresponding to one value of u:

$$\begin{array}{cccccc} 1, & 2, & 4, & 8, & 16, & 11 \\ 3, & 6, & 12, & 3, & 6, & 12 \end{array}$$

We thus get nine distinct residue classes and $R(m,t) = 9$. The number of information places is $k = 21 - 9 = 12$ and we get a 2 error-correcting binary group code (21, 12). To actually construct the code, we have to compute

$$f(y) = (y - x^3)(y - x^6)(y - x^{12})(y - x^{24})$$
$$(y - x^{48})(y - x^{33})(y - x^9)(y - x^{18})(y - x^{36})$$

where x is a primitive element of $GF(2^6)$. A minimum function of $GF(2^6)$ is $x^6 + x + 1$. Hence, using the relation $x^6 + x + 1 = 0$, the coefficients of the polynomial $f(y)$ will be all reduced to 0 and 1. The 2^{12} message sequences will be the 21-place binary vectors corresponding to the elements of the ideal generated by $f(y)$ in R_{21}. $\bar{V}(M^*)$ is the ideal generated by

$$\bar{f}(y) = (y^{21} - 1)/\bar{f}(y)$$
$$= y^{12} + y^{11} + y^9 + y^7 + y^3 + y^2 + y + 1.$$

Hence the parity check matrix A^* can be taken as

$$A^* = \|\beta_1 \vdots \beta_2 \vdots \cdots \beta_9\|$$

where β_i' is the (1×21) reversed vector corresponding to $y^{i-1}\bar{f}(y)$,

$i = 1, 2, \cdots, 9$. A 2 error-correcting (21, 12) code has also been studied by Prange (1958).

Example 2. Let $n = 73$. Then $c = 7$, $m = 9$. Let $t = 4$. The residue classes corresponding to the integer $2^j u (u = 1,3,5,7; 0 \leqq j \leqq 8)$ can be exhibited as

1,	2,	4,	8,	16,	32,	64,	55,	37
3,	6,	12,	24,	48,	23,	46,	19,	38
5,	10,	20,	40,	7,	14,	28,	56,	39
7,	14,	28,	56,	39,	5,	10,	20,	40.

The third and the fourth rows in this scheme are identical. Hence $R(m,t) = 27$ and $k = 46$. We thus get a 4 error-correcting binary group code (73, 46). This 4 error-correcting (73, 46) group code has also been obtained by Prange (1959).

Example 3. Let $n = 85$. Then $c = 3$, $m = 8$. Let $t = 6$. The residue classes corresponding to the integers $2^j u (u = 1,3,5,7,9,11; 0 \leqq j \leqq 7)$ can be exhibited as

1	2	4	8	16	32	64	43
3	6	12	24	48	11	22	44
5	10	20	40	80	75	65	45
7	14	28	56	27	54	23	46
9	18	36	72	59	33	66	47
11	22	44	3	6	12	24	48

The rows corresponding to $u = 3$ and 11 coincide. Hence $R(m,t) = 40$ and $k = 45$. We thus get a 6 error-correcting binary group code (85, 45).

SECTION III

We shall now discuss a method which enables us to get matrices possessing the property (P_{2t}) by adjoining other matrices. For the purpose of this section the subscripts carried by a matrix will denote the number of rows and columns of the matrix. Thus, $A_{n,r}$ denotes a matrix with n rows and r columns. $O_{n,r}$ will denote a matrix with n rows and r columns, each of whose elements is zero. Also $O_{n,1}$ will denote a column vector with n zero elements, and $O_{1,r}$ a row vector with r zero elements. Finally, $j_{r,1}$ will denote a column vector with r unities as elements. The elements of all the matrices considered belong to $GF(2)$.

LEMMA 3. If $A_{n,r}$ possesses the property (P_{2t}) then the matrix

$$\| A_{n,r}, \quad B_{n,s} \| \tag{7}$$

obtained from it by adjoining s new columns ($s > 0$) also possesses the property (P_{2t}).

Proof is obvious.

LEMMA 4. If the matrix $F_{n,r}$ possesses the property (P_{2t}), then the matrix

$$G_{n+1,r+1} = \left\| \begin{array}{c|c} F_{n,r} & j_{n,1} \\ \hline O_{1,r} & 1 \end{array} \right\| \tag{8}$$

possesses the property (P_{2t}).

Denote the matrix $\|F_{n,r} \vdots j_{n,1}\|$ formed by the first n rows of $G_{n+1,r+1}$ by $\bar{F}_{n,r+1}$. From Lemma 3, no $2t$ rows of $\bar{F}_{n,r+1}$ can be dependent. Again, consider the $2t$ rows obtained by choosing $2t - 1$ rows from $\bar{F}_{n,r+1}$ and adjoining the last row of $G_{n+1,r+1}$. These cannot be dependent. Otherwise the corresponding $2t - 1$ rows of $F_{n,r}$ which possess the property (P_{2t}) would be dependent. This completes the proof of the Lemma.

THEOREM 2. If the matrix $A_{n,r-r_0}$, $r > r_0$, possesses the property (P_{2t-2}) and the matrices

$$\| A_{n,r-r_0} \vdots T_{n,r_0} \| \quad \text{and} \quad F_{n',r_0+d-1} \tag{9}$$

$d \geqq 1$, possess the property (P_{2t}), then the matrix

$$M_{n+n'+1,r+d} = \left\| \begin{array}{c|c|c|c} A_{n,r-r_0} & T_{n,r_0} & O_{n,d-1} & O_{n,1} \\ \hline O_{n',r-r_0} & F_{n',r_0+d-1} & & j_{n',1} \\ \hline O_{1,r-r_0} & O_{1,r_0+d-1} & & 1 \end{array} \right\| \tag{10}$$

also possesses the property (P_{2t}).

Clearly the matrix $\bar{A}_{n,r+d}$ consisting of the first n rows of $M_{n+n'+1,r+d}$ has the property (P_{2t}). Also from Lemma 4, the matrix $\bar{G}_{n'+1,r+d}$ formed by the last $n' + 1$ rows of $M_{n+n'+1,r+d}$ has the property (P_{2t}). To prove the theorem we have to show that the $2t$ rows obtained by choosing any c rows of $\bar{A}_{n,r+d}$ and any $2t - c$ rows of $\bar{G}_{n'+1,r+d}$, $0 \leqq c \leqq 2t$, cannot be dependent. From what has been said this is true for $c = 2t$ or 0. If $c = 2t - 1$, then the last coordinate of the chosen rows adds up to unity. Hence they cannot be dependent because the matrix $A_{n,r-r_0}$ has the property (P_{2t-2}). This completes the proof of the theorem.

As in Section II, let $c = c(n)$ be the smallest integer such that $1 + cn$ is a power of 2, this power being $m = m(n)$. Let $R(m,t)$ be defined as in Lemma 2. We then have

THEOREM 3.

$$n_{2t}[R(m,t) + d] \geqq 1 + n + n_{2t}[R(m,t) - R(m,t-1) + d - 1]$$

where $n_{2t}(r)$ has been defined in the introduction, and

$$1 \leqq d < R(m+1,t) - R(m,t).$$

Let M^* be the matrix given by (2.3). We can then write

$$M^* = \| M_1^*, M_3^*, \cdots, M_u^*, \cdots, M_{2t-1}^* \|$$

where M_u^* is defined by (2.4).

Using the operations (a) and (b) described under Lemma 2, we can drop redundant columns from M^* and arrive at a matrix with n rows and $R(m,t)$ columns. Let the number of columns in the block coming from M_{2t-1}^* be r_0 and the submatrix of these columns be T_{n,r_0}. Let the number of columns coming from the part $\|M_1^*, M_3^*, \cdots, M_{2t-3}^*\|$ be $r - r_0$ and the submatrix of these columns be $A_{n,r-r_0}$. Then $r = R(m,t)$, $r - r_0 = R(m,t-1)$, and the matrices $\|A_{n,r-r_0} \vdots T_{n,r_0}\|$ and $\|A_{n,r-r_0}\|$ possess the properties (P_{2t}) and (P_{2t-2}) respectively. Let

$$r_0 + d - 1 = R(m,t) - R(m,t-1) + d - 1$$

and let

$$n' = n_{2t}(r_0 + d - 1)$$

Then there exists a matrix F_{n',r_0+d-1} with elements from $GF(2)$ and possessing the property (P_{2t}). We can now construct the matrix

$$M_{n+n'+1,r+d}$$

given by (3.4). The required result then follows from Theorem 2.

The most useful case of Theorem 3 is when $c = 1$, $n = 2^m - 1$. For this case we have

COROLLARY (1). $n_{2t}[R(m,t) + d] \geqq 2^m + n_{2t}[R(m,t) - R(m,t-1) + d - 1]$ A less powerful but simpler result is

COROLLARY (2). $n_{2t}(mt + d) \geqq 2^m + n_{2t}(m + d - 1)$

This follows by applying our reasoning to M^* without dropping any redundant column.

Example 4. Let us consider the case $t = 2$, $c = 1$, so that $n = 2^m - 1$. Then $R(m,2) = 2m$ and corollary (2) gives the same result as corollary (1). We know that $n_4(2m) \geqq 2^m - 1$. But one may want to get a bound on $n_4(2m+1)$. From corollary (2) we have

$$n_4(2m+1) \geqq 2^m + n_4(m)$$

For example,

(i) $$n_4(21) \geqq 2^{10} + n_4(10)$$
$$\geqq 2^{10} + 2^5 - 1$$

(ii) $$n_4(15) \geqq 2^7 + n_4(7)$$
$$\geqq 2^7 + 2^3 + n_4(3)$$
$$\geqq 2^7 + 2^3 + 3$$

SECTION IV

It is easy to see by exhaustive trial that $n_4(m) = m$ for $m = 1,2,3$; $n_4(4) = 5$, $n_4(5) = 6$, and $n_4(6) = 8$. Similarly, we can easily see that $n_{2t}(m) = m$ for $m = 1, 2, \cdots 2t$; $n_6(7) = 8$ and $n_{12}(13) = 14$. Using these facts and the results we have obtained, we can construct the following table where $L_{2t}(r)$ denotes the number of vectors in V_r that we can actually obtain such that no $2t$ are dependent. Thus $L_{2t}(r)$ is a lower bound for $n_{2t}(r)$.

The three asterisks in Table I indicate those cases corresponding to

TABLE I

$t = 1$		$t = 2$		$t = 3$		$t = 4$		$t = 5$		$t = 6$	
r	$L_2(r)$	r	$L_4(r)$	r	$L_6(r)$	r	$L_8(r)$	r	$L_{10}(r)$	r	$L_{12}(r)$
2	3	6	7	6	7	14	15	25	31	30	31
3	7	7	11	7	8	15	20	26	37	31	37
4	15	8	15	8	9	16	21	27	63	32	38
5	31	9	21*	9	10	17	22	28	67	33	63
6	63	10	31	10	15	18	23	29	68	34	70
7	127	11	36	11	18	19	24	30	69	35	71
		12	63	12	19	20	31	31	70	36	72
		13	71	13	20	21	37	32	71	37	73
		14	127	14	21	22	38	33	72	38	74
				15	31	23	39	34	73	39	75
				16	37	24	63	35	127	40	85*
				17	38	25	70			41	86
				18	63	26	71			42	127
				19	70	27	73*				
				20	72	28	127				
				21	127						

the three examples given after Theorem 1. Given n and t, $n \leqq 100$, $t \leqq 6$, we can find out from Table I the maximum possible k for which we can obtain by our methods a t-error correcting (n,k) group code. For this purpose we need to use the fact that if $n_{2t}(r) = n$, then for any positive integer c we have a t-error correcting $(n - c, n - r - c)$ group code. Thus, for instance, if we are seeking the largest value of k for $n = 90$, $t = 4$, we shall note that $L_8(27) < 90 < L_8(28)$ and decide that the required value of k is $90 - 28 = 62$.

RECEIVED: February 23, 1960.

REFERENCES

BOSE, R. C., AND RAY-CHAUDHURI, D. K. (1960). On a class of error correcting binary group codes. *Information and Control* **3**, 68.

PETERSON, W. W. (1960) Encoding and error-correction procedures for Bose-Chaudhuri codes. To appear in *IRE Trans. on Inform. Theory*.

PRANGE, E. (1958). Some cyclic error-correcting codes with simple decoding algorithms. Tech. note AFCRC-TN-58-156, Air Force Cambridge Research Center, Bedford, Massachusetts.

PRANGE, E. (1959). The use of coset equivalence in the analysis and decoding of group codes. Tech. Rept. AFCRC-TR-59-164, Air Force Cambridge Research Center, Bedford, Massachusetts.