J. H. Griesmer

A Bound for Error-Correcting Codes

Abstract: This paper gives two new bounds for the code word length n which is required to obtain a binary group code of order 2^k with mutual distance d between code words. These bounds are compared with previously known bounds, and are shown to improve upon them for certain ranges of k and d. Values of k and d are given for which one of these bounds can actually be achieved; in such cases, the structure of the resulting codes is shown to satisfy a certain condition.

1. Introduction

This paper deals with the class of error-correcting codes called *group codes*, and examines the problem of determining the *minimum code word length* n, or equivalently, the *minimum number of check positions* $n - k$, which are necessary for a group code to have a given error-correcting ability. The basic paper of Hamming [1] gives a lower bound on minimum number of check positions which is quite sharp for low values of $n/(n-k)$, i.e., for codes which have a *low redundancy* or transmit information at a *high rate*. Improvements have been made on the Hamming bound for higher redundancy codes [2, 3, 4]. The present paper gives two lower bounds which are a further improvement on the Hamming bound for the case of higher redundancy group codes. These bounds are derived in Section 2, and are compared with previous results in Section 3. Section 4 contains two theorems on the existence and structure of group codes for which one of the bounds is actually attained.

We begin by introducing some of the basic notions in the theory of error-correcting binary codes which we shall require. A sequence of n binary digits is called a *code word*. Two code words are said to have *mutual distance* d, if they differ in exactly d out of n positions [1]. A set S of code words is called an *e-error-correcting code* [1], if any two code words have mutual distance at least $d = 2e + 1$. If the members of S form a group under the operation of digitwise modulo 2 addition, we say S is a *group code* [5]. In this case, S has order 2^k, $k \leq n$. Our interest is in group codes of order 2^k having mutual distance at least d between code words; we shall term such a code a (k, d) *group code*, for short. Because of the group property, the requirement that any two code words have mutual distance at least d is equivalent to the requirement that all nonzero code words contain at least d ones, i.e., have *weight* at least d, since the mutual distance between code words is precisely the weight of that code word which is their sum.

We shall assume that a group code of order 2^k and code word length n is obtained by forming a $k \times n$ *generator matrix* [6], consisting of k independent vectors of length n, whose components are binary digits, and combining these k vectors in all possible ways to generate the set of $2^k - 1$ nonzero code words. This set, together with the sequence of n zeros, forms a group code of order 2^k. Any group code can be generated in this way.

Each column of a $k \times n$ generator matrix is one of $2^k - 1$ different types of columns, where a *column of type* j, $j = 1, 2, \cdots, 2^k - 1$, is a column of k binary digits which is the binary representation of the integer j, considering the top entry as the units digit and proceeding downward. Any generator matrix, and, hence, any group code, can be described, within a permutation of columns, by giving the number of columns of each type which occur in the matrix: $N = (n_1, n_2, \cdots, n_{2^k-1})$. This is Slepian's *modular representation* [5].

The weights of the $2^k - 1$ nonzero code words of a group code of order 2^k can be obtained by multiplying the vector N by a $2^k - 1 \times 2^k - 1$ matrix C_k [3, 6]

$$W = C_k N^T, \tag{1.1}$$

where W^T is a $(2^k - 1)$-component vector:

$$W^T = (w_1, w_2, \cdots, w_{2^k-1}),$$

with $w_i = w_{2^{p_1-1}+2^{p_2-1}+\cdots+2^{p_r-1}}$ designating the weight of the code word formed by combining r rows of the generator matrix indexed by $k \geq p_1 > p_2 > \cdots > p_r \geq 1$, $1 \leq r \leq k$. We shall say, for short, w_i *is the weight of the* i^{th} *code word*, $i = 1, 2, \cdots, 2^k - 1$. Using this convention for W requires that the matrix C_k have its entries defined as follows:

$$c_{ij} = \begin{cases} 1 \text{ if the number of places where } (i)_2 \text{ and } (j)_2 \\ \quad \text{have ones in common is odd,} \\ 0 \text{ otherwise,} \end{cases}$$

where $(i)_2$ and $(j)_2$ denote the binary representation of integers i and j, respectively, $1 \leq i, j \leq 2^k - 1$. For example, if

$$G = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

is a generator matrix of a group code of order 2^3, it has modular representation $N = (1, 0, 1, 0, 1, 1, 1)$. The set of nonzero code words indexed by $i = 1, \cdots, 7$ which are generated by the rows of G are the following:

$i = 1$: 1 1 1 0 1

$i = 2$: 0 1 0 1 1

$i = 3$: 1 0 1 1 0

$i = 4$: 0 0 1 1 1

$i = 5$: 1 1 0 1 0

$i = 6$: 0 1 1 0 0

$i = 7$: 1 0 0 0 1

The weight w_i of the i^{th} code word can be calculated directly, or by using (1.1),

$$W = C_3 N^T = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \\ 3 \\ 3 \\ 3 \\ 2 \\ 2 \end{bmatrix}.$$

Our aim will be to work in the reverse direction from (1.1), viz., given a weight vector $W^T = (w_1, w_2, \cdots, w_i, \cdots, w_{2^k-1})$, with $w_i \geq 1$, find a vector $N = (n_1, n_2, \cdots, n_j, \cdots, n_{2^k-1})$ satisfying the inequality system

$$C_k N^T \geq W. \tag{1.2}$$

Such a vector N will be the modular representation of a group code of order 2^k, where the i^{th} code word has weight at least w_i. That the resulting group code has order 2^k, i.e., that the resulting generator matrix consists of k linearly independent rows, is immediate, since any dependence among generator rows would imply $w_i = 0$ for some i. In particular, since our interest is in (k, d) group codes, i.e., each nonzero code word is required to have weight at least d, we shall use for W^T a $(2^k - 1)$-component vector with each component equal to d.

Our object will be to study (k, d) group codes of minimum length. We define $N(k, d)$ as *the minimum code word length required for a* (k, d) *group code.* Given k and d, an integer program can be formulated whose solution is the modular representation of a (k, d) group code of minimum length, so that the code word length for this code is $N(k, d)$:

$$\text{Minimize} \quad n = \sum_{j=1}^{2^k-1} n_j$$

subject to

$$\sum_{j=1}^{2^k-1} c_{ij} n_j \geq d \qquad i = 1, \cdots, 2^k - 1, \tag{1.3}$$

$$n_j \geq 0, \quad \text{integral} \quad j = 1, \cdots, 2^k - 1.$$

A vector $N = (n_1, n_2, \cdots, n_j, \cdots, n_{2^k-1})$ which is a solution to this integer program is the modular representation of the desired minimum length (k, d) group code.

An equivalent integer program for finding a (k, d) group code of minimum length was given by McCluskey [2]. The formulation there differs slightly from (1.3) in the indexing of code words and column types, and in the specification of the first k columns of the generator matrix, leaving only the remaining $n - k$ columns to be determined. Following Ref. [6], we can state this second assumption as a requirement that the generator matrix is in "reduced echelon form." Any generator matrix can be put into this form by premultiplication by a suitable nonsingular matrix and postmultiplication by a suitable permutation matrix.

2. Lower bounds on $N(k, d)$

We use the inequality system for the integer program (1.3) to deduce a result relating $N(k, d)$ and $N\{k - 1, [(d + 1)/2]\}$, where $[(d + 1)/2]$ means "the greatest integer less than or equal to $(d + 1)/2$." We first prove three lemmata.

• *Lemma 1*

i) $c_{ij} = c_{2^{k-1}+i,j}$, $\quad i = 1, \cdots, 2^{k-1} - 1,$ $\quad j = 1, \cdots, 2^{k-1} - 1,$

ii) $1 - c_{ij} = c_{2^{k-1}+i,j}$, $\quad i = 1, \cdots, 2^{k-1} - 1,$ $\quad j = 2^{k-1}, \cdots, 2^k - 1.$

• *Proof*

i) $(i)_2$ and $(2^{k-1} + i)_2$ have the same number of ones in common with $(j)_2$, when $1 \leq i, j \leq 2^{k-1} - 1$. ii) $(2^{k-1} + i)_2$ has an additional one in common with $(j)_2$, as compared with $(i)_2$, when $1 \leq i \leq 2^{k-1} - 1$, $2^{k-1} \leq j \leq 2^k - 1$.

• *Lemma 2*

Let S_k be a (k, d) group code in which at least one code word has exactly weight d. Then there exists a generator matrix G for S_k in which this code word is the k^{th} generator row.

• *Proof*

Let G' be any generator matrix for the code S_k, and assume that a code word which has weight exactly d is the sum of r rows of G' indexed by $1 \leq p_1 < p_2 < \cdots < p_r \leq k$, $1 \leq r \leq k$. If we premultiply G' by the nonsingular matrix K which adds the generator rows indexed by $p_1, p_2, \cdots, p_{r-1}$ to the row indexed by p_r, we obtain the equivalent generator matrix $G = KG'$ with a code word having weight exactly d as its $p_r{}^{\text{th}}$ row, $1 \leq p_r \leq k$. A simple interchange of the $p_r{}^{\text{th}}$ row of G with the k^{th} row of G will make this code word the k^{th} generator.

• *Lemma 3*

Let S_k be a (k, d) group code in which at least one code word has exactly weight d, and let a generator matrix G be chosen for the code S_k so that this row is the k^{th} generator row. Let n_i be the number of columns of type j, $j = 1, \cdots, 2^k - 1$, in G. Then

$$\sum_{i=1}^{2^{k-1}-1} c_{ij} n_j \geq [(d+1)/2] \qquad i = 1, \cdots, 2^{k-1} - 1.$$

• *Proof*

We have

$$\sum_{j=1}^{2^{k-1}} c_{ij} n_j \geq d \qquad i = 1, \cdots, 2^k - 1. \tag{2.1}$$

Adding the i^{th} inequality to the $(2^{k-1} + i)^{\text{th}}$, $i = 1, \cdots, 2^{k-1} - 1$, and using Lemma 1, we obtain

$$2 \cdot \sum_{j=1}^{2^{k-1}-1} c_{ij} n_j + \sum_{j=2^{k-1}}^{2^{k-1}} n_j \geq 2d \qquad i = 1, \cdots, 2^{k-1} - 1. \tag{2.2}$$

We have assumed the k^{th} generator row, i.e., the $(2^{k-1})^{\text{st}}$ code word, has weight exactly d. Hence,

$$\sum_{j=1}^{2^{k-1}} c_{2^{k-1},j} n_j = \sum_{j=2^{k-1}}^{2^{k-1}} n_j = d,$$

since

$$c_{2^{k-1},j} = \begin{cases} 0 & 1 \leq j < 2^{k-1} \\ 1 & 2^{k-1} \leq j \leq 2^k - 1. \end{cases}$$

Upon substitution in (2.2), we obtain

$$\sum_{j=1}^{2^{k-1}-1} c_{ij} n_j \geq d/2 \qquad i = 1, \cdots, 2^{k-1} - 1. \tag{2.3}$$

Since the left-hand side of (2.3) is an integer, we may strengthen the right-hand side to

$$\sum_{j=1}^{2^{k-1}-1} c_{ij} n_j \geq I(d/2) \qquad i = 1, \cdots, 2^{k-1} - 1, \tag{2.4}$$

where $I(x/p)$ denotes "the least integer greater than or equal to x/p." Now $I(x/p) = [(x + p - 1)/p]$. Hence,

$$\sum_{j=1}^{2^{k-1}-1} c_{ij} n_j \geq [(d+1)/2] \qquad i = 1, \cdots, 2^{k-1} - 1. \tag{2.5}$$

• *Theorem 1*

$$N(k, d) \geq d + N\{k - 1, [(d+1)/2]\}. \tag{2.6}$$

• *Proof*

Let S_k be a (k, d) group code of minimum length, i.e., S_k has code word length $n = N(k, d)$. Clearly, at least one code word of S_k has exactly weight d, since otherwise S_k would not have minimum length. Let G be a generator matrix for S_k in which the k^{th} generator row of G has exactly weight d. Let n_j be the number of columns of type j, $j = 1, \cdots, 2^k - 1$, in G.
Then

$$N(k, d) = n = \sum_{j=1}^{2^{k-1}} n_j = d + \sum_{j=1}^{2^{k-1}-1} n_j. \tag{2.7}$$

From Lemma 3,

$$\sum_{j=1}^{2^{k-1}-1} c_{ij} n_j \geq [(d+1)/2] \qquad i = 1, \cdots, 2^{k-1} - 1. \tag{2.8}$$

Hence, the $(2^{k-1} - 1)$-component vector $(n_1, n_2, \cdots, n_{2^{k-1}-1})$ is the modular representation of a $\{k - 1, [(d+1)/2]\}$ group code. Hence

$$\sum_{i=1}^{2^{k-1}-1} n_i \geq N\{k-1, [(d+1)/2]\}. \tag{2.9}$$

Combining (2.7) and (2.9), we obtain (2.6).

Theorem 1 can now be applied $k-1$ times to obtain one bound on $N(k, d)$.

• *Theorem 2*

$$N(k, d) \geq \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i]. \tag{2.10}$$

• *Proof*

$$\begin{aligned}
N(k, d) &\geq d + N\{k-1, [(d+1)/2]\} \\
&\geq d + [(d+1)/2] \\
&\quad + N\{k-2, [\{[(d+1)/2]+1\}/2]\} \\
&= d + [(d+1)/2] \\
&\quad + N\{k-2, [(d+3)/4]\} \\
&\quad \vdots \\
&\geq \sum_{i=0}^{p-1} [(d + 2^i - 1)/2^i] \\
&\quad + N\{k-p, [(d + 2^p - 1)/2^p]\} \\
&\quad \vdots \\
&\geq \sum_{i=0}^{k-2} [(d + 2^i - 1)/2^i] \\
&\quad + N\{1, [(d + 2^{k-1} - 1)/2^{k-1}]\} \\
&= \sum_{i=0}^{k-2} [(d + 2^i - 1)/2^i] \\
&\quad + [(d + 2^{k-1} - 1)/2^{k-1}] \\
&= \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i],
\end{aligned}$$

using the fact that $N(1, d) = d$.

Theorem 2 provides a sharp lower bound on $N(k, d)$ when d is large compared with k. Section 4 discusses minimum length codes which achieve this bound for values of d satisfying $d \geq 2^{k-2} - 1$.

As an example of the use of Theorem 2, we compute a bound on code word length for a group code of order 2^5 which corrects three errors:

$$\begin{aligned}
N(5, 7) &\geq 7 + N(4, 4) \\
&\geq 7 + 4 + N(3, 2) \\
&\geq 11 + 2 + N(2, 1) \\
&\geq 13 + 1 + N(1, 1) \\
&\geq 14 + 1 = 15.
\end{aligned}$$

For d fixed, when $k \geq 1 + \log_2 (d-1)$, the bound (2.10) assumes a simpler form. Let $||(d-1)_2||$ denote the number of ones in the binary representation of $d-1$, i.e., the weight or norm of $(d-1)_2$. Then, using the relation

$$\sum_{i=0}^{\infty} [(d-1)/2] = 2(d-1) - ||(d-1)_2||,$$

we have

$$\begin{aligned}
N(k, d) &\geq \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i] \\
&= \sum_{i=0}^{k-1} [(d-1)/2^i] + k \qquad (2.11) \\
&= \sum_{i=0}^{\infty} [(d-1)/2^i] + k \\
&= 2(d-1) - ||(d-1)_2|| + k.
\end{aligned}$$

The bound (2.11) increases at the same rate as k, for a fixed d. Yet the results of Hamming [1] give a lower bound on $N(k, d)$:

$$\begin{aligned}
&N(k, d = 2e+1) \\
&\qquad \geq \min \left\{ n \left| \left[2^n / \sum_{i=0}^{e} \binom{n}{i} \right] \geq 2^k \right. \right\} \qquad (2.12) \\
&N(k, d = 2e+2) \\
&\qquad \geq 1 + \min \left\{ n \left| \left[2^n / \sum_{i=0}^{e} \binom{n}{i} \right] \geq 2^k \right. \right\},
\end{aligned}$$

which increases slightly faster than k. Thus, for fixed d, as k becomes large, (2.11) becomes more slack than (2.12). We shall compare these bounds in more detail in the next section. We shall also see in the next section that combined use of (2.6) and (2.12) provides a better lower bound on $N(k, d)$, for certain values of k and d, than either (2.10), i.e., (2.11), or (2.12) alone.

We complete this section by using (2.12) for the cases $d = 3$ and $d = 4$ to improve (2.10) or (2.11) for d in the range $3 \leq d \leq 2^{k+1}$. We shall make use of the fact, as shown by Hamming, that (2.12) actually becomes an equality for $d = 3$ and $d = 4$.

• *Theorem 3*

i) If $2^{k-p} + 1 \leq d < 2^{k-p} + 2^{k-p-1} + 1$, where $0 \leq p \leq k-1$, then

$$\begin{aligned}
N(k, d) \geq &\sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] \\
&+ \min \{n \,|[2^n/(n+1)] \geq 2^{p+1}\}. \qquad (2.13)
\end{aligned}$$

ii) If $2^{k-p} + 2^{k-p-1} + 1 \leq d < 2^{k-p+1} + 1$, where $0 \leq p \leq k-1$, then

$$N(k, d) \geq \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + 1 + \min \{n \mid [2^n/(n+1)] \geq 2^{p+1}\}. \quad (2.14)$$

• *Proof*

i) $$N(k, d) \geq d + N\{k-1, [(d+1)/2]\}$$
$$\vdots$$
$$\geq \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + N\{p+1, [(d + 2^{k-p-1} - 1)/2^{k-p-1}]\}$$
$$= \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + N(p+1, 3)$$
$$= \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + \min \{n \mid [2^n/(n+1)] \geq 2^{p+1}\}.$$

ii) $$N(k, d) \geq d + N\{k-1, [(d+1)/2]\}$$
$$\vdots$$
$$\geq \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + N\{p+1, [(d + 2^{k-p-1} - 1)/2^{k-p-1}]\}$$
$$= \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + N(p+1, 4)$$
$$= \sum_{i=0}^{k-p-2} [(d + 2^i - 1)/2^i] + 1 + \min \{n \mid [2^n/(n+1)] \geq 2^{p+1}\}.$$

Table 1 gives the values of the lower bounds on $N(k, d)$ provided by Theorems 2 and 3 for the cases $k \leq 16$ and odd d satisfying $5 \leq d \leq 25$. Equation (2.10) is used whenever $d \geq 2^{k+1} + 1$, and (2.13) and (2.14) are used otherwise. Table 1 is divided into three sections: (2.10) is used to compute the bound in Section I; (2.10) and (2.13)-(2.14) produce an equivalent bound in Section II; (2.13)-(2.14) is used in Section III. The bound for d even is one more than the bound for $d - 1$. As an example, using (2.14),

$$N(12, 7) \geq 7 + N(11, 4)$$
$$= 7 + 1 + \min \{n \mid [2^n/(n+1)] \geq 2^{11}\}$$
$$= 7 + 1 + 15 = 23.$$

Hence, as does (2.12), (2.14) shows that a code word length of at least 23 is required in order to obtain a (12, 7) group code, i.e., a group code of order 2^{12} which is 3-error correcting.

3. Comparison of lower bounds on $N(k, d)$

McCluskey [2] has shown that, for $d \geq k$,

$$N(k, d) \geq I[(2^k - 1)d/2^{k-1}], \quad (3.1)$$

and for $d < k$,

$$N(k, d) \geq I\left[(2^k - 1)\, d/2^{k-1} + 2^{1-k} \sum_{s=d+1}^{k} \binom{k}{s}(s - d)\right]. \quad (3.2)$$

(3.1) can also be derived from the work of MacDonald [3]. We show in Theorem 4 that (2.10) improves on (3.1) when $d \geq k$, and on (3.2) when $d < k$. We use an alternative form for (2.10) in Theorem 4, viz.,

$$N(k, d) \geq \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i] = \sum_{i=0}^{k-1} I(d/2^i). \quad (3.3)$$

• *Theorem 4*

i) For $d \geq k$,

$$I[(2^k - 1)d/2^{k-1}] \leq \sum_{i=0}^{k-1} I(d/2^i). \quad (3.4)$$

ii) For $d < k$,

$$I\left[(2^k - 1)d/2^{k-1} + 2^{1-k} \sum_{s=d+1}^{k} \binom{k}{s}(s - d)\right] \leq \sum_{i=0}^{k-1} I(d/2^i). \quad (3.5)$$

• *Proof*

i) *Case A.* $d = h2^{k-1}$, $h \geq 1$.

In this case, both left- and right-hand sides of (3.4) are equal to $h(2^k - 1)$.

Case B. $d = h2^{k-1} + 2^{j_1} + 2^{j_2} + \cdots + 2^{j_p}$, where $k - 2 \geq j_1 > j_2 > \cdots > j_p \geq 0$, $h \geq 0$. On the one hand,

$$I[(2^k - 1)d/2^{k-1}] = I(2d - d/2^{k-1}) = 2d - h$$

On the other hand,

$$\sum_{i=0}^{k-1} I(d/2^i) \geq h \sum_{i=0}^{k-1} 2^{k-1-i} + \left(\sum_{i=0}^{j_1} 2^{j_1-i} + 1\right) + \left(\sum_{i=0}^{j_2} 2^{j_2-i} + 1\right) + \cdots + \left(\sum_{i=0}^{j_p} 2^{j_p-i} + 1\right)$$
$$= h(2^k - 1) + 2^{j_1+1} + 2^{j_2+1} + \cdots + 2^{j_p+1}$$
$$= 2(h2^{k-1} + 2^{j_1} + 2^{j_2} + \cdots + 2^{j_p}) - h$$
$$= 2d - h,$$

since $I(d/2^i)$ has a contribution 2^{j_r-i} from 2^{j_r},

Table 1 **A lower bound on $N(k, d)$**

$1 \leq k \leq 16$, $5 \leq$ odd $d \leq 25$

d \ k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
5	5	8	10	11	12	14	15	16	17	18	19	20	22	23	24	25
7	7	11	13	14	15	17	18	19	20	21	22	23	25	26	27	28
9	9	14	17	19	20	21	23	24	25	26	27	28	29	31	32	33
11	11	17	20	22	23	24	26	27	28	29	30	31	32	34	35	36
13	13	20	24	26	27	28	30	31	32	33	34	35	36	38	39	40
15	15	23	27	29	30	31	33	34	35	36	37	38	39	41	42	43
17	17	26	31	34	36	37	38	40	41	42	43	44	45	46	48	49
19	19	29	34	37	39	40	41	43	44	45	46	47	48	49	51	52
21	21	32	38	41	43	44	45	47	48	49	50	51	52	53	55	56
23	23	35	41	44	46	47	48	50	51	52	53	54	55	56	58	59
25	25	38	45	49	51	52	53	55	56	57	58	59	60	61	63	64
Section	I			II				III								

$1 \leq r \leq p$, if $i \leq j_r$, and has a contribution $+1$ from 2^{i_r}, $1 \leq r \leq p$, if $i = j_r + 1$.

ii) It can be shown that, if $d < k$,

$$I\left[(2^k - 1)d/2^{k-1} + 2^{1-k} \sum_{s=d+1}^{k} \binom{k}{s}(s - d)\right] \leq I[(2^d - 1)d/2^{d-1}] + k - d;$$

we omit the argument. Using (3.4) for the case $k = d$, we have the following chain of inequalities:

$$\begin{aligned} I\left[(2^k - 1)d/2^{k-1} + 2^{1-k} \sum_{s=d+1}^{k} \binom{k}{s}(s - d)\right] &\leq I[(2^d - 1)d/2^{d-1}] + k - d \\ &\leq \sum_{i=0}^{d-1} I(d/2^i) + k - d \\ &\leq \sum_{i=0}^{k-1} I(d/2^i), \end{aligned}$$

which gives (3.5).

The bound (3.1) is relatively sharp for even $d \geq k$. This fact can be used to improve the bound for $d - 1$, by subtracting 1 from the bound for d. The first time that (3.1) does not produce a bound for an even d which is as good as that given by (2.10) or (3.3) is when $d = 10$. Here, for $k = 4$, (3.1) gives

$$N(4, 10) \geq I((2^4 - 1)10/2^3) = 19,$$

while (2.10) gives

$$N(4, 10) \geq 10 + 5 + 3 + 2 = 20.$$

We shall use Theorem 4 in comparing the condition on k provided by (2.10) with one appearing in the work of Plotkin [4]. He showed

$$A(n, d) \leq \left[\frac{2d}{2d - n}\right]_{\text{even}} \qquad 2d > n, \tag{3.6}$$

where $A(n, d)$ is the maximum number of binary sequences of length n which have mutual distance at least d, and $[x]_{\text{even}}$ denotes "the greatest *even* integer less than or equal to x." If (3.6) is applied to group codes, it states that

$$2^k \leq \left[\frac{2d}{2d - n}\right]_{\text{even}} \qquad 2d > n. \tag{3.7}$$

This bound can also be obtained from (3.1):

$$n \geq I[(2^k - 1)d/2^{k-1}] \geq (2^k - 1)d/2^{k-1}$$
$$\Rightarrow n/d \geq 2 - 2^{1-k}$$
$$\Rightarrow 2^{k-1} \leq d/(2d - n)$$
$$\Rightarrow 2^k \leq 2d/(2d - n)$$
$$\Rightarrow 2^k \leq [2d/(2d - n)]_{\text{even}}.$$

Hence, the condition (2.10) or (3.3) on k

$$n \geq \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i]$$
$$= \sum_{i=0}^{k-1} I(d/2^i) = k + \sum_{i=0}^{k-1} [(d - 1)/2^i]$$

is stronger than that provided by (3.7), because of Theorem 4.

The work of Plotkin can also be used to provide a condition on k when $2d \leq n$. For this case, in addition to (3.6), we also use [4]

$$A(n, d) \leq 2A(n - 1, d) \tag{3.8}$$

and repeat its use $(n - 2d + 1)$ times to obtain:

$$A(n, d) \leq 2^{n-2d+1} A(2d - 1, d). \tag{3.9}$$

Now, by (3.7),

$$A(n, d) \leq 2^{n-2d+1}[2d/\{2d - (2d - 1)\}]_{\text{even}} \leq d2^{n-2d+2}. \tag{3.10}$$

When (3.10) is applied to group codes, it states that

$$2^k \leq d2^{n-2d+2} \qquad 2d \leq n. \tag{3.11}$$

We now show that (2.10) or (3.3) provides a stronger condition on k than (3.11). We first treat in detail the case $n = 2d$. Let p be defined by $2^p \leq d < 2^{p+1}$. Then (3.11) reduces to $k \leq p + 2$. We now evaluate (2.10) or (3.3) for $k = p + 2$, and show that it is at least as large as $n = 2d$:

$$\sum_{i=0}^{p+1} [(d + 2^i - 1)/2^i]$$
$$= (p + 2) + \sum_{i=0}^{p+1} [(d - 1)/2^i]$$
$$= (p + 2) + 2(d - 1) - ||(d - 1)_2||$$
$$= 2d + p - ||(d - 1)_2||$$
$$\geq 2d,$$

since $d - 1 < 2^{p+1} - 1$ implies that $||(d - 1)_2|| < p + 1$. Hence, when $n = 2d$, (2.10) or (3.3) is as strong a condition on k as (3.11). Now the bound (3.11) on k increases at the same rate as n. However, the condition (2.10) or (3.3) on k increases at the same rate as n only for $k \geq 1 + \log_2 (d - 1)$. For $k < 1 + \log_2 (d - 1)$ it increases at a slower rate than n. Hence, for a fixed d, since (2.10) or (3.3) is as strong a condition on k as (3.11) when $n = 2d$, it remains as strong as (3.11) for all $n \geq 2d$.

We now present an example comparing the use of (3.11) with (2.10). Let $d = 5$ and $n = 10$. Then, using (3.11), $2^k \leq 5 \cdot 2^2$ or $k \leq 4$. Using (2.10), we see that k can be at most 3, since

$$\sum_{i=0}^{2} [(d + 2^i - 1)/2^i] = 5 + 3 + 2 = 10.$$

Finally, we compare the bounds (2.10), (2.13), and (2.14) with the Hamming bound (2.12). As already noted in the last section, for k sufficiently large, (2.12) provides a sharper bound than (2.10). For small k, the bound (2.12) can be improved upon, using (2.10), (2.13), or (2.14). Furthermore, for certain values of k and d, by using (2.6), and substituting the best bound for $N\{k - 1, [(d + 1)/2]\}$, we can improve on (2.12). For example, in the case $k = 18$, $d = 13$, from (2.12) we have

$$N(18, 13) \geq 41.$$

However, by (2.6),

$$N(18, 13) \geq 13 + N(17, 7)$$
$$\geq 13 + 29 = 42,$$

since (2.12) gives $N(17, 7) \geq 29$. Table 2 gives a summary of when (2.12) can be improved upon for odd values of d from 5 up to 21. It lists the largest value of k for which an improvement can be made upon (2.12), and the smallest value of k for which (2.12) provides a better bound on $N(k, d)$ than either (2.10), (2.13), (2.14), or the use of (2.6) and a bound for $N\{k - 1, [(d + 1)/2]\}$. In each case, the corresponding bound is given.

4. Codes which achieve the bound (2.10) and their structure

In Theorem 5, we present (k, d) group codes which achieve the bound (2.10) and, thus, are minimum length codes. In all cases, $d \geq 2^{k-2} - 1$.

• *Theorem 5*

For the following values of d, the lower bound (2.10),

$$N(k, d) \geq \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i],$$

can be achieved by a (k, d) group code:

Table 2 **Comparison of lower bounds on $N(k, d)$**

$5 \leq$ odd $d \leq 21$

d	*Largest k for which an improvement upon (2.12) can be made*	*Corresponding n*	*Smallest k for which (2.12) is best*	*Corresponding n*
5	14	23	23	33
7	8	19	18	31
9	25	43	33	52
11	18	38	23	44
13	35	62	43	71
15	27	56	33	63
17	45	81	52	88
19	37	75	48	88
21	55	100	68	115

i) $d = h2^{k-1} + 2^{k-2} + 2^{k-3} + \cdots + 2^{k-p} + 1$

$d = h2^{k-1} + 2^{k-2} + 2^{k-3} + \cdots + 2^{k-p} + 2$

$$\begin{cases} h \geq 0 \\ 2 \leq p \leq k-1 \end{cases}$$

ii) $d = (h+1)2^{k-1} - 2^{k-p} - 1$

$= h2^{k-1} + 2^{k-2} + \cdots + 2^{k-p} - 1$

$d = (h+1)2^{k-1} - 2^{k-p}$

$= h2^{k-1} + 2^{k-2} + \cdots + 2^{k-p}$

$$\begin{cases} h \geq 0 \\ 2 \leq p \leq k-1. \end{cases}$$

• *Proof*

We treat only the case of odd d. The even case follows from the well-known result that a $(k, 2t)$ group code can always be obtained from a $(k, 2t-1)$ group code by adding one additional column.

i) Let n_j, the number of columns of type j used in forming the code, be defined as follows:

$$n_j = \begin{cases} h & \text{if } j \leq 2^{k-p+1} - 1, \text{ but } j \neq 2^r, \\ & 0 \leq r \leq k-p, \\ h+1 & \text{otherwise.} \end{cases}$$

We first observe that, since a column of type 2^r, $r = 0, \cdots, k-1$, occurs at least once in the generator matrix, its k rows are independent and the resulting code will be of order 2^k.
We must now show

$$\sum_{j=1}^{2^k-1} n_j = \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i], \tag{4.1}$$

and

$$\sum_{j=1}^{2^k-1} c_{ij} n_j \geq d \qquad i = 1, \cdots, 2^k - 1. \tag{4.2}$$

We first evaluate the left-hand side of (4.1):

$$\sum_{j=1}^{2^k-1} n_j = \sum_{j=2^{k-p+1}}^{2^k-1} n_j + \sum_{\substack{j=2^r \\ r=0,\cdots,k-p}} n_j + \sum_{\substack{j=3 \\ j\neq 2^r}}^{2^{k-p+1}-1} n_j$$

$$= (h+1)(2^{k-p+1} + 2^{k-p+2} + \cdots + 2^{k-1})$$
$$+ (h+1)(k-p+1)$$
$$+ h[1 + 3 + \cdots + (2^{k-p} - 1)]$$
$$= h(2^k - 1) + 2^{k-p+1} + 2^{k-p+2}$$
$$+ \cdots + 2^{k-2} + 2^{k-1} + (k-p+1).$$

Listing the sum on the right-hand side of (4.1) term by term, we have:

$$
\begin{aligned}
\sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i] = {} & h2^{k-1} && + 2^{k-2} && + 2^{k-3} && + \cdots + 2^{k-p+1} && + 2^{k-p} && + 1 && (i = 0) \\
& + h2^{k-2} && + 2^{k-3} && + 2^{k-4} && + \cdots + 2^{k-p} && + 2^{k-p-1} && + 1 && (i = 1) \\
& \quad \vdots \\
& + h2^{k-1-i} && + 2^{k-2-i} && + 2^{k-3-i} && + \cdots + 2^{k-p+1-i} && + 2^{k-p-i} && + 1 && (i < k - p) \\
& \quad \vdots \\
& + h2^{p} && + 2^{p-1} && + 2^{p-2} && + \cdots + 2 && + 1 && + 1 && (i = k - p) \\
& + h2^{p-1} && + 2^{p-2} && + 2^{p-3} && + \cdots + 1 && + 1 && && (i = k - p + 1) \\
& \quad \vdots \\
& + h2 && + 1 && && && && && (i = k - 2) \\
& + h && + 1 && && && && && (i = k - 1) \\
& = h(2^k - 1) && + 2^{k-1} && + 2^{k-2} && + \cdots + 2^{k-p+2} && + 2^{k-p+1} && + (k - p + 1).
\end{aligned}
$$

To show (4.2), we observe that $\sum_{i=1}^{2^k-1} c_{ij}n_i$ receives weight $h2^{k-1}$ from h occurrences of each column type, since C_k has 2^{k-1} ones in each row. We must now calculate the contribution to each $\sum_{i=1}^{2^k-1} c_{ij}n_i$ of one each of column types 1, 2, 4, $\cdots$, 2^{k-p}, and 2^{k-p+1}, $\cdots$, $2^k - 1$.

• *Case A.*

If $(i)_2$ does not have ones appearing in digits indexed 1, 2, 4, $\cdots$, 2^{k-p}, then, for this i, $c_{ij} = 0$ for $j < 2^{k-p+1}$, so that all 2^{k-1} ones in this row occur after the $(2^{k-p+1})^{st}$ column. Hence

$$\sum_{j=1}^{2^k-1} c_{ij}n_j = h2^{k-1} + 2^{k-1} = (h + 1)2^{k-1} \geq d$$

where i satisfies one of $i \equiv 2^{k-p+1} \pmod{2^{k-p+2}}$, $i \equiv 2^{k-p+2} \pmod{2^{k-p+3}}$, $\cdots$, $i \equiv 2^{k-2} \pmod{2^{k-1}}$, $i = 2^{k-1}$.

• *Case B.*

If $(i)_2$ has a one in at least one of the digits indexed 1, 2, 4, $\cdots$, 2^{k-p}, then, for this i, $\sum_{j=1}^{2^k-1} c_{ij}n_j$ receives at least weight 1 from columns of type 1, 2, 4, $\cdots$, 2^{k-p}. Furthermore, it receives weight 2^{k-p} from columns of type j, $2^{k-p+1} \leq j \leq 2^{k-p+2} - 1$, weight 2^{k-p+1} from columns of type j, $2^{k-p+2} \leq j \leq 2^{k-p+3} - 1$, $\cdots$, weight 2^{k-1} from columns of type j, $2^{k-1} \leq j \leq 2^k - 1$, so that

$$\sum_{i=1}^{2^k-1} c_{ij}n_i \geq h(2^{k-1}) + 2^{k-2} + \cdots + 2^{k-p+1} + 2^{k-p} + 1 = d$$

for all such i.

ii) These codes are given explicitly by McCluskey [2] and MacDonald [3]. We give the modular representation for the general case, following MacDonald:

$$n_j = \begin{cases} h & \text{if } 1 \leq j \leq 2^{k-p+1} \\ h + 1 & \text{if } 2^{k-p+1} + 1 \leq j \leq 2^k - 1. \end{cases}$$

That the code given by this modular representation is actually a (k, d) group code with code word length equal to $N(k, d)$, can be demonstrated in a manner similar to (i). We omit the argument.

As examples of the range of Theorem 5, for $k = 5$, minimum length codes are given for $d \geq 7$, $d \equiv 7$, $\cdots$, 16 (mod 16). For $k = 6$, minimum length codes are given for $d \geq 15$, $d \equiv 15$, $\cdots$, 18 (mod 32) and $d \equiv 23$, $\cdots$, 32 (mod 32).

For the case $k = 5$, Table 3 gives an explicit code for the distances $d = 7$, 9, 11, 13, 15, based on Theorem 5. The table states which part of the theorem is used in constructing the codes. For each code, we have $n_j = 1$, for $17 \leq j \leq 31$, and so the table lists only the values of n_j for $1 \leq j \leq 16$.

Finally, we give a result on the structure of (k, d) group codes which achieve the bound (2.10). If an integer $h \geq 0$ is defined by

$$h2^{k-1} \leq d - 1 < (h + 1)2^{k-1},$$

then any column type is used at most $h + 1$ times in such a code. When $h = 0$, i.e., $d < 2^{k-1} + 1$, this means that such a code uses a column of each type at most once. We first need:

• *Theorem 6*

If $N(k, d) = \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i]$,

Table 3 **Minimum length codes**

$k = 5$, $d = 7, 9, 11, 13, 15$

d \ j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	*Part of Theorem 5 used*
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	(ii)
9	1	1	0	1	0	0	0	1	0	0	0	0	0	0	0	1	(i)
11	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	(ii)
13	1	1	0	1	0	0	0	1	1	1	1	1	1	1	1	1	(i)
13	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	(ii)
15	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	(i)

then

$$N(k-1, d) = \sum_{i=0}^{k-2} [(d + 2^i - 1)/2^i]$$
$$= N(k, d) - [(d + 2^{k-1} - 1)/2^{k-1}].$$

• *Proof*

Let $h \geq 0$ be the integer defined by

$$h2^{k-1} \leq d - 1 < (h+1)2^{k-1}.$$

Then $[(d + 2^{k-1} - 1)/2^{k-1}] = h + 1$. We shall prove the theorem by taking a $k \times n$ generator matrix G for a (k, d) group code with code word length $n = N(k, d)$, and deriving a $k - 1 \times n - h - 1$ generator matrix G' for a $(k - 1, d)$ group code.

We may assume that G has been put in reduced echelon form, $G = [I_k \mid M]$, where I_k is the identity matrix of order k, and M is a $k \times n - k$ matrix. We have

$$n - k = \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i] - k$$
$$= \sum_{i=0}^{k-1} \{[(d + 2^i - 1)/2^i] - 1\}$$
$$= \sum_{i=0}^{k-1} [(d-1)/2^i]$$
$$\geq \sum_{i=0}^{k-1} [h2^{k-1}/2^i]$$
$$= \sum_{i=0}^{k-1} h2^{k-1-i}$$
$$= h(2^k - 1).$$

Since there are $2^k - 1$ different types of columns, each type of column must be used at least h times to form M, or one type of column is used at least $h + 1$ times to form M. In the first case, we will have at least h occurrences of the column of type 2^{k-1} (in fact, exactly h occurrences). Dropping these h columns, together with the one column of this type in I_k, and then eliminating the k^{th} row of G, we obtain a submatrix

$$G' = [I_{k-1} \mid M']$$

which is clearly the generator matrix of a $(k - 1, d)$ group code. The code word length is

$$n' = n - h - 1 = \sum_{i=0}^{k-2} [(d + 2^i - 1)/2^i].$$

In the second case, we may assume, without loss of generality, that a column of type j, with $j \geq 2^{k-1}$, occurs at least $h + 1$ times in M. Let this type of column have ones in rows $i_1, \cdots, i_r$ and in row k. We may premultiply G by a nonsingular matrix K which adds the last row of G to the rows indexed $i_1, \cdots, i_r$. The result, a generator matrix H equivalent to G, has the appearance

$$H = \left[\begin{array}{c|c|c} I_{k-1} & A & M' \\ \hline 0 & & \end{array}\right],$$

where A is a $k \times 1$ matrix, i.e., a column vector, with ones in rows $i_1, \cdots, i_r$ and k, and M' is a $k \times n - k$ matrix with at least $h + 1$ columns of type 2^{k-1} (in fact, exactly $h + 1$ columns of type 2^{k-1}). As in the first case, we drop these $h + 1$ columns, plus the k^{th} row, and obtain a generator

matrix for a $(k - 1, d)$ group code with code word length

$$n' = n - h - 1 = \sum_{i=0}^{k-2} [(d + 2^i - 1)/2^i].$$

• *Corollary 1*

If $N(k, d) = \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i]$, then any generator matrix for a (k, d) group code of length $n = N(k, d)$ uses a column of type j, $j = 1, \cdots, 2^k - 1$, at most $h + 1$ times, where $h \geq 0$ is the integer defined by $h2^{k-1} \leq d - 1 < (h + 1)2^{k-1}$.

• *Proof*

Assume a column of type j is used more than $h + 1$ times. Without loss of generality, we may assume $j \geq 2^{k-1}$. Then an equivalent generator matrix can be obtained which contains more than $h + 1$ columns of type 2^{k-1}, by premultiplying by a suitable nonsingular matrix. Then the submatrix obtained by dropping the columns of type 2^{k-1} and the k^{th} row of the generator matrix is a generator matrix for a $(k - 1, d)$ code with code word length

$$\begin{aligned} n' < n - h - 1 &= N(k, d) - h - 1 \\ &= \sum_{i=0}^{k-1} [(d + 2^i - 1)/2^i] \\ &\quad - [(d + 2^{k-1} - 1)/2^{k-1}] \\ &= N(k - 1, d), \end{aligned}$$

which is a contradiction.

Acknowledgment

The author is grateful to A. B. Fontaine, W. W. Peterson, and J. L. Selfridge for their help and advice on the subjects in this paper. He would also like to express his thanks to R. E. Gomory for his interest in the computational aspects of the problem of finding minimum-length codes through the method of integer programming.

References

[1] R. W. Hamming, *Bell System Tech. J.*, **29**, 147-160 (1950).
[2] E. J. McCluskey, *Bell System Tech. J.*, **38**, 1485-1512 (1959).
[3] J. E. MacDonald, *IBM Journal*, **4**, 43-57 (1960).
[4] M. Plotkin, *IRE Transactions on Information Theory*, **IT-6**, 445-450 (1960).
[5] D. Slepian, *Bell System Tech. J.*, **35**, 203-234 (1956).
[6] A. B. Fontaine, and W. W. Peterson, *IRE Transactions on Information Theory*, **IT-5**, Special Supplement, 60-70 (May, 1959).

Received April 1, 1960