On Linear Unequal Error Protection Codes

BURT MASNICK, MEMBER, IEEE, AND JACK WOLF, MEMBER, IEEE

Abstract—The class of codes discussed in this paper has the property that its error-correction capability is described in terms of correcting errors in specific digits of a code word even though other digits in the code may be decoded incorrectly. To each digit of the code words is assigned an error protection level f_i. Then, if f errors occur in the reception of a code word, all digits which have protection f_i greater than or equal to f will be decoded correctly even though the entire code word may not be decoded correctly.

Methods for synthesizing these codes are described and illustrated by examples. One method of synthesis involves combining the parity check matrices of two or more ordinary random error-correcting codes to form the parity check matrix of the new code. A decoding algorithm based upon the decoding algorithms of the component codes is presented. A second method of code generation is described which follows from the observation that for a linear code, the columns of the parity check matrix corresponding to the check positions must span the column space of the matrix.

Upper and lower bounds are derived for the number of check digits required for such codes. The lower bound is based upon counting the number of unique syndromes required for a specified error-correction capability. The upper bound is the result of a constructive procedure for forming the parity check matrices of these codes. Tables of numerical values for the upper and lower bounds are presented.

Introduction

ALMOST all algebraic codes previously considered in the literature have the property that their error-correction capabilities are described in terms of correcting errors in code words rather than in correcting errors in individual digits of a code word. For example, a "t error correcting code" will decode to the correct code word if t or fewer errors occur in the transmitted word.

In this paper, codes are investigated in which certain digits of a code word are protected against a greater number of errors than other digits in the code word. Specifically, assigned to each digit of the code words is an error protection level, denoted f_i. Then if f errors occur in the transmission of a code word, all digits for which $f_i \geq f$ will be decoded correctly even though the entire word may be decoded incorrectly. Such codes will be called *u*nequal *e*rror *p*rotection codes (UEP codes).

Manuscript received June 20, 1966; revised February 20, 1967. An abbreviated version of this paper was presented at the Mohawk Valley Communications Symposium (NATCOM), October 11–13, 1965. The research in this work was supported by United States Air Force of Scientific Research Grant AF-AFOSR-499-65 and Contract AF-49-(638) 1600.

B. Masnick is with the Research Department, Grumman Aircraft Engineering Corporation, Bethpage, L. I., N. Y. 11714. He was formerly with the Department of Electrical Engineering, New York University, Bronx, N. Y.

J. Wolf is with the Department of Electrical Engineering, Polytechnic Institute of Brooklyn, Brooklyn, N. Y. He was formerly with the Department of Electrical Engineering, New York University, Bronx, N. Y.

An example where UEP codes may find application is in the transmission of binary coded decimal digits. Consider the binary coded decimal representation of an integer M whose magnitude may vary between 0 and $2^\beta - 1$.

$$M = m_{\beta-1}2^{\beta-1} + m_{\beta-2}2^{\beta-2} + \cdots + m_0$$

where $m_i = 0$ or 1. M can be represented by the coefficients m_i as

$$m_{\beta-1}m_{\beta-2} \cdots m_0.$$

If an error changed the coefficient $m_{\beta-1}$, the magnitude of M would be changed by $2^{\beta-1}$. On the other hand, if an error changed the digit m_0, the magnitude of M would be changed by 1. Thus if errors of large magnitude are more important (costly) than errors of small magnitude, it may be desirable to seek a coding scheme that provides more protection for the high-order digits than for the low-order digits.

In some circumstances it may be advisable to vary the amount of error protection from block of digits to block of digits. Consider the problem of an observer transmitting the results of many simultaneous experiments (as from a satellite). Some of the experiments may be more important than others and therefore may be deserving of higher-error protection. While this could be accomplished by using a separate code for each experiment, it would usually be more efficient and more desirable to use one code, and thus one encoder and one decoder.

This paper contains an analysis of the problem of linear codes[1] for which the protection afforded each digit or set of digits can be different from the protection afforded some other digit or set of digits.

Previous approaches to this problem include the work of Gray,[6] Bedrosian,[4] Bellman and Kalaba,[5] and Buchner.[7] Gray proposed a kind of magnitude protection code with no redundancy for the problem of analog to digital conversion of position data. Bedrosian and Bellman and Kalaba analyzed weighted PCM systems where greater signal amplitude and power are allocated to the higher-order binary digits. Buchner considered sending information with some information digits encoded by a Hamming single-error-correcting code and other information digits uncoded. He also evolved a figure of merit for such schemes.

Theory of UEP Codes

Sufficient conditions for the generation of *u*nequal *e*rror *p*rotection codes, hereafter called UEP codes, are presented in the following theorems.

The discussion is mainly concerned with the properties of the parity check matrix[1] H of UEP codes. Consider those digits corresponding to the columns of H which are linearly dependent on $2f_i$ or $2f_i + 1$ (but no fewer) other columns of H. Call these digits f_i protected. Denote by f_1 the lowest protection level and by f_s the highest protection level and adopt the convention that f_j is $f_1 + j - 1$.[1] Vector quantities will have a bar above as in $\bar{v}$. The ith column of H will be denoted $\bar{h}_i$ and the syndrome[1] of a vector $\bar{v}$ will be denoted $S(\bar{v})$. Unless otherwise stated, the results discussed hold for nonbinary as well as binary codes so that, in general, the components of all vectors and matrices will be elements from a finite field containing q elements.

Theorem 1

Consider a code V which consists of all vectors in the null space of a parity check matrix H. The code V can correct any pattern of weight f_1 or less. In addition, if any error pattern of weight f_i or less occurs, any f_i or greater protected digit can be decoded correctly.

Proof: Since no linear dependence relation involving fewer than $2f_1 + 1$ columns can exist, the code V must be able to correct any error of weight less than or equal to f_1.

Let $\omega(\bar{E})$ be the Hamming weight of the vector $\bar{E}$. To prove the second part of the theorem it is sufficient to show that the syndrome of any error pattern $\bar{E}_1$, $0 < \omega(\bar{E}_1) \leq f_i$, which contains an error in the pth digit which is f_i protected is unique from both 1) the syndrome of any error pattern $\bar{E}_2$, $0 \leq \omega(\bar{E}_2) \leq f_i$, which does not include an error in the pth digit, and 2) the syndrome of any error pattern $\bar{E}_3$, $0 \leq \omega(\bar{E}_3) \leq f_i$, which contains a different error in the pth digit.[2]

Let $\bar{v}$ be any code word in V

$$\bar{E}_1 = [e_{11}, e_{12}, e_{13}, \cdots, e_{1p} \neq 0, \cdots, e_{1n}]$$

$$\bar{E}_2 = [e_{21}, e_{22}, e_{23}, \cdots, e_{2p} = 0, \cdots, e_{2n}]$$

$$\bar{E}_3 = \left[e_{31}, e_{32}, e_{33}, \cdots, e_{3p} \neq \begin{cases} 0 \\ e_{1p} \end{cases}, \cdots, e_{3n}\right].$$

Then

$$S(\bar{v}) = \bar{0}, \quad S(\bar{v} + \bar{E}_1) = S(\bar{E}_1), \quad S(\bar{v} + \bar{E}_2) = S(\bar{E}_2),$$

so that

$$S(\bar{E}_1) = \sum_{i=1}^{n} e_{1i}\bar{h}_i \quad \text{and} \quad S(\bar{E}_2) = \sum_{i=1}^{n} e_{2i}\bar{h}_i.$$

Assume there exists an error pattern $\bar{E}_1$ and an error pattern $\bar{E}_2$ such that $S(\bar{E}_1) = S(\bar{E}_2)$. Then

$$\sum_{i=1}^{n} (e_{1i} - e_{2i})\bar{h}_i = \bar{0}.$$

Since $e_{1p} \neq 0$ and $e_{2p} = 0$, then a set of at most $2f_i$ columns of H including the column $\bar{h}_p$ is linearly dependent, contrary to hypothesis. Therefore the assumption that the error patterns $\bar{E}_1$ and $\bar{E}_2$ can be found such that $S(\bar{E}_1) = S(\bar{E}_2)$ is false.

Assume there exists an error pattern $\bar{E}_1$ and an error pattern $\bar{E}_3$ such that $S(\bar{E}_1) = S(\bar{E}_3)$. Then

$$\sum_{i=1}^{n} (e_{1i} - e_{3i})\bar{h}_i = \bar{0}.$$

Since e_{3p} is unequal to both 0 and e_{1p}, then a set of at most $2f_i - 1$ columns of H, including the column $\bar{h}_p$ is linearly dependent, contrary to hypothesis. Therefore, the assumption that error patterns $\bar{E}_1$ and $\bar{E}_3$ can be found such that $S(\bar{E}_1) = S(\bar{E}_3)$ is false.

Thus if any error pattern of weight less than or equal to f_i occurs which involves the pth digit, the syndrome will specify the particular error which occurred in this pth digit. Also if an error pattern of weight less than or equal to f_i occurs which does not involve the pth digit, the fact that the pth digit is correct can be determined from the syndrome. Therefore, the theorem is proved.

The codes described in Theorem 1 have the following properties. If an error pattern of weight no greater than f_i but greater than f_1 involves the pth digit, the syndrome will identify the error in the pth digit, thereby permitting the correction of this digit. However, some incorrect digits may remain incorrect and some correct digits may be erroneously "corrected" to become incorrect digits. This can occur since the syndrome may be the same as the syndrome of some other error pattern of weight less than or equal to f_i that has the same error in the pth digit. For example let $\bar{E}_1$ and $\bar{E}_2$ be given as

$$\bar{E}_1 = [e_{11}, e_{12}, \cdots, e_{1p} \neq 0, \cdots, e_{1n}],$$

$$f_1 < \omega(\bar{E}_1) \leq f_i,$$

and

$$\bar{E}_2 = [e_{21}, e_{22}, \cdots, e_{2p} = e_{1p}, \cdots, e_{2n}],$$

$$f_i < \omega(E_2) \leq f_i.$$

If $S(\bar{E}_1) = S(\bar{E}_2)$ then

$$\sum_{i=1}^{n} (e_{1i} - e_{2i})\bar{h}_i = \bar{0}.$$

Let t be the number of nonzero terms in this summation. Then, there is a set of t linearly dependent columns of H which does *not* include the column $\bar{h}_p$. Since t is at most $2f_i - 2$, so long as $2f_1 < t \leq 2f_i - 2$ and none of the t columns corresponds to a digit that is $[t/2]$ or greater protected, it is possible for $S(\bar{E}_1)$ to be the same as $S(\bar{E}_2)$. (The notation $[x]$ indicates the integer part of x.)

It can also be true that if an error pattern of weight greater than f_1 but no greater than f_i occurs which does not involve the pth digit, the resulting syndrome may erroneously indicate an incorrect error pattern but will not indicate an error in the pth digit.

The following theorem considers conditions for an entire word to be decoded correctly.

[1] Note that for some values of j there may be no digits which are $f_j = f_1 + j - 1$ protected.

[2] This condition need not be considered for binary codes since only one type of error can then occur in any digit.

Theorem 2

Let there be a linear group code with t_1 digits f_1 protected, t_2 digits f_2 protected, $\cdots$, t_z digits f_z protected. In addition to the digit protection discussed in Theorem 1, any error pattern can be corrected provided that there are f_j or fewer errors in the f_j or less protected digits, $j = 1, 2, \cdots, z$.

Proof: It will be sufficient to show that the syndrome of any error pattern $\bar{E}_1$ which satisfies the above conditions is unique from: 1) the syndrome of any other error pattern $\bar{E}_2$ which also satisfies the above conditions, and 2) the syndrome of any error pattern, $\bar{E}_3$, not necessarily satisfying the above condition, where $\omega(\bar{E}_3) \leq \omega(\bar{E}_1)$ and $\bar{E}_3$ is distinct from $\bar{E}_1$.

Assume error patterns $\bar{E}_1$ and $\bar{E}_2$ exist such that $S(\bar{E}_1) = S(\bar{E}_2)$. Therefore,

$$\sum_{i=1}^{n} (e_{1i} - e_{2i})\bar{h}_i = \bar{0}.$$

Since $\bar{E}_1$ and $\bar{E}_2$ differ, there must be a most highly protected digit in which they differ. Assume that the most highly protected digit in which $\bar{E}_1$ and $\bar{E}_2$ differ is μ protected. By hypothesis, $\bar{E}_1$ and $\bar{E}_2$ may each have no more than μ errors in digits that are μ or less protected. Therefore, the relation above describes a set of at most 2μ columns of H, including one that corresponds to a μ protected digit, which is linearly dependent, contrary to hypothesis. Therefore, no most highly protected digit in which $\bar{E}_1$ and $\bar{E}_2$ differ can be found and hence if $S(\bar{E}_1) = S(\bar{E}_2)$, then $\bar{E}_1 = \bar{E}_2$.

Suppose error patterns $\bar{E}_1$ and $\bar{E}_3$ exist such that

$$S(\bar{E}_1) = S(\bar{E}_3).$$

Then

$$\sum_{i=1}^{n} (e_{1i} - e_{3i})\bar{h}_i = \bar{0}.$$

Let $\omega_1 = \omega(\bar{E}_1)$, $\omega_3 = \omega(\bar{E}_3)$. Assume the most highly protected digit in which E_1 and E_3 disagree is μ protected. Let E_1 and E_3 agree in ψ nonzero digits which are μ or greater protected. Therefore, there are at most $\omega_1 - \psi$ nonzero e_{1i} that do not sum to zero with corresponding e_{3i}. There can be at most $\omega_3 - \psi$ nonzero e_{3i} that are not summed to zero by corresponding e_{1i}. But $\omega_1 - \psi \leq \mu$, and since $\omega_3 \leq \omega_1$ we know $\omega_3 - \psi \leq \mu$. Thus the summation above indicates that there exists a set of 2μ or fewer columns of H, including a column corresponding to a μ protected digit which is linearly dependent, contrary to hypothesis. Hence there can be no highest protected digit in which $\bar{E}_1$ and $\bar{E}_3$ differ and therefore no error patterns $\bar{E}_1$ and $\bar{E}_3$ can be found such that $S(\bar{E}_1) = S(\bar{E}_3)$. Therefore, the theorem is proved.

Coset Decoding

Consider the decoding of a linear binary group code, to be used with the binary symmetric channel, by using the standard array[1] as a decoding table. Then the probability of correct decoding is as large as possible if each coset leader is chosen to have the minimum weight in its coset. These coset leaders are the correctable error patterns. The question now arises as to whether the use of the correctable error patterns of a UEP code as coset leaders would lead to a situation where a coset leader would not be the minimum weight vector in its coset, thereby producing a smaller probability of correct decoding. Two vectors are in the same coset if, and only if, their syndromes are equal. Theorem 2 guarantees that no correctable error pattern has the same syndrome as any other error pattern of the same or lower weight. Therefore, coset decoding of a UEP code where the coset leaders are chosen to be the known correctable error patterns will lead to minimum probability of error decoding.

Another question to be considered is the minimum error protection requirement of the check digits in a UEP code. This question arises when one contemplates the generation of codes with highly protected information digits and little protected check digits. The check columns are linearly independent (as shown in Masnick[8]), and thus each check digit is involved in some linear dependence relation involving information digits. Therefore, each check digit is as protected as the least protected information digit with which it is involved in a linear dependence relation.

A Simple UEP Code and a Generalization

In order to provide extra error protection for *one* digit in a group code one must make the column of the H matrix corresponding to that digit be of "higher linear independence" than the other columns of H. One method of accomplishing this for binary codes is to add a number of ones to the chosen column and add on a number of columns so that every column is involved in at least one linear dependence relation. The process is illustrated below. We start with the H matrix for a Hamming binary single-error correcting (7, 3) group code[1]

$$H = \begin{array}{c} \begin{matrix} c_1 & c_2 & m_1 & c_3 & m_2 & m_3 & m_4 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}.$$

Protection against any two errors involving digit m_4 is provided by changing H to H' where:

$$H' = \begin{array}{c} \begin{matrix} c_1 & c_2 & m_1 & c_3 & m_2 & m_3 & m_4 & c_4 & c_5 \end{matrix} \\ \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix} \end{array}.$$

For the V' corresponding to H', the digits m_4, c_4, and

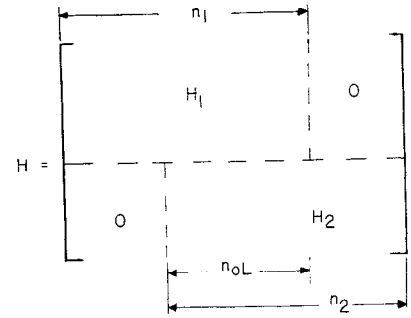

Fig. 1. Check matrix with overlapping submatrices.

c_5 are protected against 2 errors and the digits c_1, c_2, m_1, c_3, m_2, and m_3 are protected against single errors.

This technique can be generalized as follows. Let there be two check matrices with elements from $GF(q)$; H_1 with n_1 columns and random error-correcting capacity e_1, and H_2 with n_2 columns and random error capacity e_2, where $e_2 \leq e_1$. Let H_1 and H_2 be joined as submatrices of H where H_1 and H_2 overlap, as shown in Fig. 1. The composite matrix H has $n_1 + n_2 - n_{0L}$ columns. Let $n_{0L} \leq e_2$.

Theorem 3

The code V for which H is the check matrix will protect the first $n_1 - n_{0L}$ digits against at least e_1 errors, the last $n_2 - n_{0L}$ digits against at least e_2 errors and the n_{0L} middle digits against at least $e_1 + e_2 - [(n_{0L} - 1)/2]$ errors.

Proof: Every column in the first $n_1 - n_{0L}$ columns of H is involved in no linear dependence relation involving $2e_1$ or fewer columns. Every column in the last $n_2 - n_{0L}$ columns of H is involved in no linear dependence relation involving $2e_2$ or fewer columns. Therefore, the first $n_1 - n_{0L}$ digits are protected against at least e_1 errors and the last $e_2 - n_{0L}$ digits are protected against at least e_2 errors.

Consider the jth column (from the left) of the n_{0L} overlapping columns. This column is involved in a linear dependence relation involving at least $2e_1$ other columns of H_1 and at least $2e_2$ other columns of H_2. Since n_{0L} is less than or equal to e_2, the jth column must be involved in a linear dependence relation involving at least $2e_2 + 1 - j$ columns to its right and at least $2e_1 - n_{0L} + j$ columns to its left or at least $2e_1 + 2e_2 + 1 - n_{0L}$ other columns of H. Since the jth column was typical of the n_{0L} middle columns, the n_{0L} middle digits are protected against at least $e_1 + e_2 - [(n_{0L} - 1)/2]$ errors.

Theorem 3 provides the basis for creating codes with three different degrees of error protection depending upon the two matrices originally chosen and on the number of overlapping columns. For example using this method one can always provide protection against one more error for one information digit by adding on two extra check digits. In this case $e_2 = 1$ and $n_{0L} = 1$. More general techniques involving the overlapping of more than two matrices can be developed.

Provided in the following is a decoding procedure for binary overlap codes which makes use of the individual decoding algorithms for the component codes with check matrices H_1 and H_2. (It is assumed that efficient decoding algorithms are available for the component codes as would be the case for BCH codes.) The proof of the validity of this procedure is given elsewhere.[8] This proof is long and is hence omitted from this paper.

Consider the occurrence of $e + \beta$ errors in a code word from an e error-correcting linear group code. This occurrence is referred to as overloading the H matrix for the code. Using syndrome decoding, one of three circumstances may result.

1) The correct error is indicated.
2) An incorrect error is indicated.
3) An unrecognizable syndrome is generated, indicating an overload of the H matrix.

In an overlap code the parity check matrices H_1 and H_2 are considered as the encoding and decoding matrices for the first n_1 and n_2 digits, respectively, of each code word. They may be used to compute the *apparent* errors in the first n_1 and n_2 digits. If these two apparent errors agree in the n_{0L} middle digits, and the weight requirements specified in Theorem 3 are met, the error has been determined.

However, the possibility exists that either H_1 or H_2 or both are overloaded. In these events, further steps are necessary. If either H_1 or H_2 is overloaded, and a recognizable syndrome results, the apparent errors will either not satisfy Theorem 3 or they will not agree in the n_{0L} middle digits. On perceiving this the procedure is to subtract from the received vector the apparent error in the n_{0L} middle digits as determined by H_1. Recompute the syndromes and apparent errors. If the apparent errors now satisfy Theorem 3 and the apparent error in the n_{0L} middle digits is $\bar{0}$ according to H_2, the error has been determined. The actual error in the first n_1 digits is the apparent error obtained in the first pass by H_1. The actual error in the last $n_2 - n_{0L}$ digits is the apparent error obtained in the second pass by H_2. If the new apparent errors do not satisfy Theorem 3, the procedure is to subtract from the received vector the apparent error in the n_{0L} middle digits as originally determined by H_2 and proceed as above. If this does not yield an error pattern that satisfies Theorem 3, both H_1 and H_2 are overloaded. In that event, complement the middle n_{0L} digits in the received vector. Then decoding with H_1 and H_2 must give the correct errors in the first $n_1 - n_{0L}$ digits and the last $n_2 - n_{0L}$ digits. The errors in the middle n_{0L} digits are then readily determined.

The Basis Method of Code Generation[9]

A procedure is shown in the following for constructing UEP codes, based upon the observation[9] that the ρ columns of the parity check matrix corresponding to the ρ check positions must form a basis for the column space. Choose k the number of information digits, and b_i the error protection for the ith information digit,

$$H = \begin{array}{c} \begin{matrix} c_1 & c_2 & c_3 & c_4 & c_5 & c_6 & c_7 & c_8 & c_9 & c_{10} & c_{11} & c_{12} & c_{13} & c_{14} & c_{15} & m_5 & m_4 & m_3 & m_2 & m_1 \end{matrix} \\ \left[\begin{matrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 \end{matrix}\right] \end{array}$$

Fig. 2. UEP check matrix constructed by basis method.

$i = 1$ to k. Choose a set of ρ linearly independent ρ-tuples to form the basis (check columns of H). Then choose a linear combination of $2b_i$ or more basis elements for the ith information column of H such that no linear combination of t columns that involves the ith information column is itself a combination of fewer than $2b_i + 1 - t$ basis vectors (check columns). The results of such a procedure are illustrated in Fig. 2. In Fig. 2 there are $k = 5$ information digits.

Digit m_1 is protected against up to 1 error

Digit m_2 is protected against up to 2 errors

Digit m_3 is protected against up to 3 errors

Digit m_4 is protected against up to 4 errors

Digit m_5 is protected against up to 5 errors.

The method of basis elements becomes difficult for more than five information digits when an attempt is made to use the fewest possible check digits.

Cyclic and Pseudo-Cyclic Codes

Since cyclic codes are very easily instrumented for encoding and decoding,[11] it is appropriate to ask if a cyclic code can provide unequal protection for the various digits. The answer, unfortunately, is no, as is shown in the following theorem.

Theorem 4

A cyclic code cannot provide greater protection from random errors for any particular digit than it does for any other digit. The proof follows by assuming that a cyclic code can provide greater protection to one digit than to another digit and proving a contradiction.

However, shortened-cyclic codes, which have much of the ease of instrumentation of cyclic codes, can be UEP codes. A hand constructed example of a binary shortened-cyclic code which can correct all single errors and all double errors that involve the x^5 digit is shown in the following.

Let the code words be all multiples of $g(x) = x^6 + x^5 + x^4 + x^2 + 1$ of degree ≤ 10. This code has five information digits and six redundant digits. Since decoding of cyclic and shortened-cyclic codes can be accomplished by dividing the altered code word by the generator polynomial and determining the error by the remainder, let us establish the remainders of the powers of x from x^0 through x^{10}.

Power of x	Remainder when divided by $g(x)$
1	1
x	x
x^2	x^2
x^3	x^3
x^4	x^4
x^5	x^5
x^6	$x^5 + x^4 + x^2 + 1$
x^7	$x^4 + x^3 + x^2 + x + 1$
x^8	$x^5 + x^4 + x^3 + x^2 + x$
x^9	$x^3 + 1$
x^{10}	$x^4 + x$

Note that the sum of the remainder of x^5 and the remainder of any other single error cannot be duplicated by the sum of any two other remainders whereas the remainder of the error $x^4 + x$ can be duplicated by the remainder of x^{10} and the remainder of the error $x^3 + x^0$ can be duplicated by the remainder of x^9.

Bounds

In this section, upper and lower bounds on the required redundancy for UEP codes are investigated.

Modified Hamming Bound[11]

By counting the number of unique syndromes necessary to achieve a specified level of error protection it is possible to give a lower bound on the number of redundant digits. Consider an (n, k) linear code over the field of q symbols, having q^{n-k} unique syndromes. Let there be t_j digits j protected, $j = 1, \cdots, s$, where

$$\sum_{j=1}^{z} t_j = n.$$

Let A_i be the number of correctable error patterns of weight i. Let T_i be the number of code digits that are i or more protected.

$$T_i = \sum_{j=i}^{z} t_j.$$

Number the code digits as follows. The z protected digits are numbered from 1 to T_z. The $z - 1$ protected digits are numbered from $T_z + 1$ to T_{z-1}, etc.

We now give a procedure to determine the A_i. We construct a "graph" of every error pattern as follows. Between $x = l$ and $x = l + 1$, we plot on the y axis the number of errors in the digit positions with numbers greater than l. For an error of weight i the graph must have the value $y = i$ between $x = 0$ and $x = 1$, and must fall to $y = 0$ at or before $x = n$. The graph of a *correctable* error pattern must be at or below $y = j$ for each set of j protected digits, which corresponds to x between T_{j-1} and T_j.

Example: Consider a code with

10 digits 1 protected,
4 digits 2 protected, and
2 digits 3 protected.

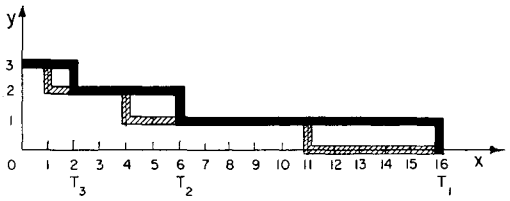

Fig. 3. Typical map of correctible error patterns.

In Fig. 3 the heavy black line represents the boundary of the graph of a correctable error pattern. The shaded line represents the map of an error pattern of weight 3 with errors in the 1st, 4th, and 11th positions. Since a one to one mapping exists between error patterns and the graphs of an error pattern, the problem of counting the number of correctable error patterns of weight 3 resolves to the problem of counting the number of graphs that begin at $y = 3$ and have $y = 0$ at $x = 16$ without going above the boundary (the thick black line) at any point. In general, we may establish the following formulas.

$$A_1 = \{T_1\}(q-1)$$

$$A_2 = \{(A_1 - 1) + (A_1 - 2) + (A_1 - 3) + \cdots + (A_1 - T_2)\}(q-1)^2$$

$$A_3 = \{[A_2 - (A_1 - 1)] + [A_2 - (A_1 - 1) - (A_1 - 2)] + \cdots + [A_2 - (A_1 - 1) - (A_1 - 2) - \cdots - (A_1 - T_3)]\}(q-1)^3$$

$$A_4 = \{\langle A_3 - [A_2 - (A_1 - 1)]\rangle + \langle A_3 - [A_2 - (A_1 - 1)] - [A_2 - (A_1 - 1) - (A_1 - 2)]\rangle + \cdots + \langle A_3 - [A_2 - (A_1 - 1)]\rangle - [A_2 - (A_1 - 1) - (A_1 - 2)] - \cdots - [A_2 - (A_1 - 1) - (A_1 - 2) - \cdots - (A_1 - T_4)]\rangle\}(q-1)^4,$$

etc.

Combining terms we find

$$A_1 = (T_1)(q-1)$$

$$A_2 = \left[T_2 \cdot A_1 - \sum_{i=1}^{T_2} i\right](q-1)^2$$

$$A_3 = \left[T_3 \cdot A_2 - \sum_{i=1}^{T_3} iA_1 + \sum_{\mu=1}^{T_3}\sum_{i=1}^{\mu} i\right](q-1)^3$$

$$A_4 = \left[T_4 \cdot A_3 - \sum_{i=1}^{T_4} iA_2 + \sum_{\mu=1}^{T_4}\sum_{i=1}^{\mu} iA_1 - \sum_{\lambda=1}^{T_4}\sum_{\mu=1}^{\lambda}\sum_{i=1}^{\mu} i\right](q-1)^4,$$

etc.

These equations are simplified using the following relations.

$$\sum_{i=1}^{T_2} i = \frac{(T_2)(T_2+1)}{2} = \binom{T_2+1}{2},$$

$$\sum_{\mu=1}^{T_3}\sum_{i=1}^{\mu} i = \sum_{\mu=1}^{T_3}\frac{\mu(\mu+1)}{2},$$

$$\sum_{\mu=1}^{T_3}\sum_{i=1}^{\mu} i = \sum_{\theta=2}^{T_3+1}\frac{(\theta)(\theta-1)}{2} = \sum_{\theta=2}^{T_3+1}\binom{\theta}{2},$$

where $\theta = \mu + 1$.

Consider the number of combinations of n things taken r at a time, denoted by $\binom{n}{r}$. This number can be divided into those combinations which do include a certain item, of which there are $\binom{n-1}{r-1}$, and those which do not include a certain item, of which there are $\binom{n-1}{r}$. Thus

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}.$$

Similarly,

$$\binom{n-1}{r} = \binom{n-2}{r-1} + \binom{n-2}{r},$$

so that $\binom{n}{r}$ can be written as

$$\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-2}{r-1} + \cdots + \binom{r-1}{r-1} = \sum_{\theta=r-1}^{n-1}\binom{\theta}{r-1}.$$

Thus

$$\sum_{\theta=2}^{T_3+1}\binom{\theta}{2} = \binom{T_3+2}{3}$$

from which it follows that

$$\sum_{\lambda=1}^{T_4}\sum_{\mu=1}^{\lambda}\sum_{i=1}^{\mu} i = \sum_{\lambda=1}^{T_4}\binom{\lambda+2}{3} = \sum_{\theta=3}^{T_4+2}\binom{\theta}{3} = \binom{T_4+3}{4}$$

and

$$\sum_{\phi=1}^{T_N}\cdots\sum_{\mu=1}^{\lambda}\sum_{i=1}^{\mu} i = \binom{T_N+N-1}{N}.$$

Thus we have

$$A_0 = 1$$

$$A_1 = T_1(q-1)$$

$$A_2 = \left[\binom{T_2}{1}A_1 - \binom{T_2+1}{2}\right](q-1)^2$$

$$A_3 = \left[\binom{T_3}{1}A_2 - \binom{T_3+1}{2}A_1 + \binom{T_3+2}{3}\right](q-1)^3$$

$$A_4 = \left[\binom{T_4}{1}A_3 - \binom{T_4+1}{2}A_2 + \binom{T_4+2}{3}A_1 - \binom{T_4+3}{4}\right](q-1)^4,$$

etc.

These equations reduce to the general form

$$A_i = \sum_{j=1}^{i} \binom{T_i + j - 1}{j} A_{i-j}(-1)^{j+1}(q-1)^j$$

where $A_0 = 1$.

Thus we have derived a recursive relationship for the number of correctable error patterns of weight i in terms of the number of correctable error patterns of weight $i-1, i-2, \cdots, 1$.

A word of caution should be mentioned concerning the use of these recursive relations. Suppose we have T_1 1 or more protected digits and $T_2 = T_1$ 2 or more protected digits. In the formulas mentioned in the foregoing T_2 must be taken to be $T_2 - 1$ since the highest numbered position on the second level of the error map could not be used. In general, if $t_i = 0$, T_i must be reduced.

Since each of the correctable error patterns must correspond to a distinct syndrome and since there are $q^{n-k} = q^r$ available syndromes, then a lower bound for the number of check digits, denoted r_L, is given as

$$r_L \geq \log_q \sum_{i=0}^{z} A_i.$$

Modified Varsharmov[10]–Gilbert[11]–Sachs[12] Bound

This bound is established by considering a procedure which must realize a linear code with the desired error correction capacity. Let us establish a code that has

1) t_1 *information* digits f_1 protected
2) t_2 *information* digits f_2 protected
. .
. .
. .
z) t_z *information* digits f_z protected.

Choose r linearly independent r-tuples. These will be the check columns for the parity check matrix. Choose t_1 r-tuples such that each is not a linear combination of any $2f_1 - 1$ or fewer previously chosen r-tuples. Choose t_2 r-tuples such that each is not a linear combination of any $2f_2 - 1$ or fewer previously chosen r-tuples.... Choose $t_z - 1$ r-tuples such that each is not a linear combination of any $2f_z - 1$ or fewer previously chosen r-tuples. We now have $n - 1$ r-tuples or columns. In the worst case, all the linear combinations mentioned above may be distinct. If q^r is greater than the number of linear combinations listed above, one more column can be added to the matrix and the code, which is the null space of this matrix, must have at least the desired properties. Let r_U be the smallest value of r such that the q^r is greater than all the linear combinations mentioned above. Then another column can be added which will correspond to the t_zth f_z protected information digit and a code with the desired properties need have no more than r_U check digits. Let

$$T_i = \sum_{j=i}^{z} t_j - 1, \qquad n = \sum_{i=1}^{z} t_i + r$$

and γ be the number of r-tuples which have been banned. Then γ can be shown to be given as

$$\begin{aligned}
\gamma = \Bigg[& 1 + \binom{n-1}{1}(q-1) + \binom{n-1}{2}(q-1)^2 + \cdots + \binom{n-1}{2f_1-1}(q-1)^{2f_1-1} \\
& + \left\{\binom{T_2}{1}\binom{n-T_2-1}{2f_2-3} + \binom{T_2}{2}\binom{n-T_2-1}{2f_2-4} + \cdots + \binom{T_2}{2f_2-2}\right\}(q-1)^{2f_2-2} \\
& + \left\{\binom{T_2}{1}\binom{n-T_2-1}{2f_2-2} + \binom{T_2}{2}\binom{n-T_2-1}{2f_2-3} + \cdots + \binom{T_2}{2f_2-1}\right\}(q-1)^{2f_2-1} \\
& + \left\{\binom{T_3}{1}\binom{n-T_3-1}{2f_3-3} + \binom{T_3}{2}\binom{n-T_3-1}{2f_3-4} + \cdots + \binom{T_3}{2f_3-2}\right\}(q-1)^{2f_3-2} \\
& + \left\{\binom{T_3}{1}\binom{n-T_3-1}{2f_3-2} + \binom{T_3}{2}\binom{n-T_3-1}{2f_3-3} + \cdots + \binom{T_3}{2f_3-1}\right\}(q-1)^{2f_3-1} \\
& + \cdots \\
& + \left\{\binom{T_z}{1}\binom{n-T_z-1}{2f_z-3} + \binom{T_z}{2}\binom{n-T_z-1}{2f_z-4} + \cdots + \binom{T_z}{2f_z-2}\right\}(q-1)^{2f_z-2} \\
& + \left\{\binom{T_z}{1}\binom{n-T_z-1}{2f_z-2} + \binom{T_z}{2}\binom{n-T_z-1}{2f_z-3} + \cdots + \binom{T_z}{2f_z-1}\right\}(q-1)^{2f_z-1} \Bigg].
\end{aligned}$$

It is known that

$$\sum_{i=0}^{\nu} \binom{A}{i}\binom{B-A}{\nu-i} = \binom{B}{\nu}.$$

Hence

$$\sum_{i=1}^{2f_j-1} \binom{T_j}{i}\binom{n-1-T_j}{2f_j-1-i} = \binom{n-1}{2f_j-1} \cdot \binom{n-1-T_j}{2f_j-1}$$

and

$$\sum_{i=1}^{2f_j-2} \binom{T_j}{i}\binom{n-1-T_j}{2f_j-2-i} = \binom{n-1}{2f_j-2} - \binom{n-1-T_j}{2f_j-2}.$$

Therefore,

$$\gamma = \sum_{i=0}^{2f_z-1} \binom{n-1}{i}(q-1)^i - \sum_{i=2}^{z} \binom{n-1-T_i}{2f_i-2}(q-1)^{2f_i-2} - \sum_{i=1}^{z} \binom{n-1-T_i}{2f_i-1}(q-1)^{2f_i-1}.$$

Thus r_U is the smallest value of r such that $q^r > \gamma$. The number r_U serves as an upper bound on the redundancy required to construct a code with given error protection specifications.

Numerical Examples of Bounds

Numerical results obtained using the upper and lower bounds are presented in Table I. The first two numbers in each row are the number of information digits which are, respectively, one error and two error protected. The third and fourth numbers in each row are, respectively, the lower and upper bounds on the number of redundant digits needed for such a code. The upper bound is realizable in the sense that it follows from a construction procedure for such codes.

Evaluation of Performance of Codes

The codes considered in this paper were motivated by the fact that in certain situations different weights (or "values of importance") should be associated with different digits of the code words. The classical method of evaluating the performance of a coding system by calculating the average probability of error for a code word is not satisfactory in these situations since all errors are weighted equally in this calculation.

Buchner[7] introduced the criterion of average numerical error for the transmissions of quantized numerical data. A generalization of this criterion termed average error cost (AEC) as discussed by Masnick[8] is defined as follows.

A "value" v_i is assigned to the jth *information* digit of each code word. Then the code word $\bar{C}_\alpha$ which contains the information digits $m_{\alpha,0}m_{\alpha,1} \cdots \alpha_{\alpha,k-1}$ is said to have the value $\sum_{i=0}^{k-1} v_i m_{\alpha,i}$.

If the code word $\bar{C}_\alpha$ is transmitted but is decoded to $\bar{C}_\beta$ at the receiver then the "cost" of this error is defined as the absolute value of the difference of these code words: i.e., $|\sum_{i=0}^{k-1} v_i m_{\alpha,i} - \sum_{i=0}^{k-1} v_i m_{\beta,i}|$.

The average error cost is then defined as the average of this quantity, the average being taken over all transmitted and received code words.

TABLE I

t_1	t_2	r_L	r_U
1	0	2	2
2	0	3	3
3	0	3	3
4	0	3	3
5	0	4	4
1	1	4	5
2	1	4	5
3	1	4	6
4	1	5	6
5	1	5	7
1	2	5	7
2	2	5	7
3	2	5	7
4	2	5	8
5	2	6	8
1	3	5	8
2	3	6	8
3	3	6	8
4	3	6	8
5	3	6	9
1	4	6	8
2	4	6	9
3	4	6	9
4	4	6	9
5	4	7	9

The details of the calculation of the AEC and numerical examples are omitted from this paper and the interested reader is referred to Masnick.[8] It should be stated, however, that the calculation involves a detailed knowledge of the structure of the code words. (The weights of all the code words are not sufficient information for this calculation.)

References

[1] W. W. Peterson, *Error-Correcting Codes.* New York: Wiley, 1961.

[2] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes," *Inform. Control*, vol. 3, pp. 279–290, 1960.

[3] Ye. V. Voronov, "Coding method for transmission of binary numbers over a noisy channel," *Radio Engrg. electronic Phys.*, vol. 8, no. 8, 1963.

[4] E. Bedrosian, "Weighted PCM," *IRE Trans. Information Theory*, vol. IT-4, pp. 45–49, March 1958.

[5] R. Bellman and R. Kalaba, "On Weighted PCM and Mean-Square Deviation," *IRE Trans. Information Theory (Correspondence)*, vol. IT-4, pp. 58–59, March 1958.

[6] F. Gray, "Pulse code modulation," U. S. Patent 2 632 058.

[7] M. M. Buchner, "Coding for numerical data transmission," Ph. D. dissertation, The Johns Hopkins University, Baltimore, Md., 1965.

[8] B. Masnic, "Unequal error protection codes," Ph.D. dissertation, New York University, New York, 1966.

[9] B. Dwork and R. Heller, "Results of a geometric approach to the theory and construction of non-binary, multiple error and failure correcting codes," *IRE Conv. Record.* pt. 4, 1959.

[10] R. R. Varsharmov, "Estimate of the number of signals in error correcting codes," *Dokl. Akad. Nauk SSSR*, vol. 117, no. 5, pp. 739–741, 1959.

[11] E. N. Gilbert, "A comparison of signalling alphabets," *Bell Sys. Tech. J.*, vol. 31, pp. 504–522, 1952.

[12] G. E. Sacks, "Multiple error correction by means of parity checks," *IRE Trans. Information Theory*, vol. IT-4, pp. 145–147, December 1958.