Coordinated Science Laboratory

UNIVERSITY OF ILLINOIS – URBANA, ILLINOIS

A DECODING METHOD FOR BOSE-CHAUDHURI BINARY CODES USING AN ERROR COUNTING TECHNIQUE

W. Jack Bouknight

REPORT-267 OCTOBER, 1965

This work was supported in part by the Joint Services Electronics Programs (U. S. Army, U. S. Navy, and U. S. Air Force) under Contract No. DA 28 043 AMC 00073(E).

Portions of this work were also supported by the National Science Foundation under Grant NSF GK-36.

A DECODING METHOD FOR BOSE-CHAUDHURI BINARY CODES USING AN ERROR COUNTING TECHNIQUE

Introduction

The first line method to solving problems in science has always been the trial and error approach. This approach is generally used until "short cuts" begin to become apparent producing end results in a more predictable manner.

As more sophisticated methods of problem solving are developed, more sophisticated tools are needed to effect these solutions. Many times, some of these tools become too unwieldy and the method must be modified to use tools more suitable to the task.

The coding, transmission, and decoding of information in the binary channel is a good example of an area beset with many problems, and many advances have been made in the development of techniques to solve these problems.

For instance, probably the simplest method of single-error detection is the simple even parity check made on an n-bit code word where the n^{th} bit is the mod 2 sum of the (n-1) bits in the rest of the code word. Hence the number of nonzero bits in the n-bit word as encoded is always even, and the occurrence of an odd number of errors will be indicated by the failure of the parity check.

A good example of a sophisticated procedure for error detection and correction is Peterson's procedure for implementation of Bose-Chaudhuri-Hocquenhem group codes[*]. These codes have very good error-correction and

---

[*] W. H. Peterson, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes," <u>IRE Trans. on Information Theory</u>, IT-6, pp. 459-470 (1960).

detection capabilities. However, the circuits needed to encode and decode information and correct as many errors as possible are quite complex because they involve arithmetic operations in Galois fields, even though the digits of the code words are binary.

In some of these methods of information coding, direct implementations of the theory may not be practical from any one of several points of view. A system may not have time to perform very complex operations in decoding, and economic reasons may put limits on the amount of hardware that may be employed in the implementation of a decoding procedure.

The method proposed here is an error correction procedure for BCH codes in which the hardware is kept simple at the expense of operating time. It is based on the property of BCH codes that information about the number of errors in a received code word is more readily obtainable, under certain conditions, than that about the location of the digits in error. The procedure involves successive tentative corrections which are accepted or rejected depending on whether the error count in the received code word has been reduced or not.

The method and the decoding logic are illustrated for a particular BCH code, the BCH (31, 16) code with an appended parity check digit, but extensions of the principle to other BCH codes are clearly possible.

Theoretical Foundations

The proposed decoding method is essentially a trial-and-error correction procedure which, like all such procedures, is straightforward in principle. However, it is critically dependent on the existence of a method to assess the effect of each trial correction. It contrasts with decoding methods which locate errors directly, e.g., Chien[*].

In the case of BCH codes, an error number detection scheme has been proposed by Kastenholz[**]. The method proposed here employs this scheme to check whether or not a given trial correction was successful in reducing the number of errors in the received code word.

The procedure will be illustrated by means of a particular BCH code. We arbitrarily select the BCH (31, 16) code over the field $GF(2^5)$ in which the minimum distance between any of the 2^{16} code points is 7. Thus, up to 3 errors can always be corrected. (Details of the development of this code are given in Appendix II.) For reasons which will become apparent later, it is advantageous to append an odd parity check digit to this code. The augmented code, the BCH (32, 16) code, can correct up to 3 errors and detect the existence of 4 errors. The odd parity of the parity check digit ensures that no transmitted code word is all zeros.

Kastenholz's error number detection scheme involves the selection of any two distinct B_m's from the formula

$$B_m = \frac{(S_1)^{2m+1} + S_{2m+1}}{S_{2m-1}}$$

where the S_j are syndromes and $m = 1,2,\ldots$ (see Appendix I). The number of errors in a code word can then be determined from the syndromes and the two B_m's as follows:

---

[*] R. T. Chien, "Cyclic Decoding Procedures for Bose-Chaudhuri-Hocquenhem Codes," IEEE Trans. on Inf. Theory, IT-10, pp. 357-363 (1964).

[**] C. E. Kastenholz, "General Purpose Computer Encoding and Decoding of Error Control Codes," NEC Proc., pp. 699-703 (1964).

for no errors, all S_j are zero

for 1 error, $B_{m1} = B_{m2} = 0$

for 2 errors, $B_{m1} = B_{m2} \neq 0$

for 3 or 4 errors, $B_{m1} \neq B_{m2}$.

In the case of the BCH (32, 16) code, more than 4 errors are of course assumed not to occur. However, the parity check digit must be used to resolve the 3 <u>or</u> 4 error indication (the parity check will fail for 3 errors, as it would for any odd number of errors, but will not fail for 4 errors), so that it is possible to distinguish the correctable cases from the case of 4 errors, which can not be corrected. This distinction is available as soon as the syndromes and the B_m functions are formed - a feature which is especially attractive in systems which retransmit uncorrectable words.

If the syndromes and the B_m functions indicate that the received code word contains 1, 2, or 3 errors, then an iterative procedure is entered which involves, at each step, (1) the tentative complementation of successive binary digits of the received code word, and (2), the application of the error number detection scheme described above to the tentatively modified code word as an acceptance criterion: If the number of errors has been reduced by the tentative complementation, an error has actually been corrected and the tentative complementation is accepted. Otherwise, it is rejected. Note that an indicated reduction of 2 or more errors can not occur for a single tentative correction.

If any step results in an error count of zero, then the remaining digits are clearly correct and can be simply copied. The procedure can similarly be terminated early when all information digits have been processed, as errors in the check digits are of no particular interest.

Implementation of the Correction Procedure for the Augmented BCH (31, 16) Code

Aside from facilities to tentatively complement and recomplement successive binary digits of the received code word, facilities must be provided to form, for each tentative correction,

a) the syndromes,

b) the two B_m functions.

In the augmented BCH (31, 16) code, three syndromes must be formed: S_1, S_3, and S_5. The two B_m functions selected are

$$B_1 = \frac{(S_1)^3 + S_3}{S_1} \quad \text{and} \quad B_2 = \frac{(S_1)^5 + S_5}{S_3} \quad .$$

Because S_1 or S_3 might become 0 during a trial correction, the B functions actually generated for comparisons with each other (and with zero) are

$$B_1 = S_3[(S_1)^3 + S_3] \text{ and } B_2 = S_1[(S_1)^5 + S_5] \ .$$

These modifications however do not affect the validity of the error number determination.

The three syndromes, derived from the received vector r(x) and the parity check matrix H^T by

$$r(x) = H^T = 0 + e(x) \cdot H^T = (S_1 \ S_3 \ S_5)$$

where e(x) is the error vector, are generated in three syndrome registers, S_1, S_3, and S_5 (see Figure 1)*, from the received code word. These syndrome registers are 5-stage cyclic shift registers arranged to perform multiplications modulo $(1 + x^3 + x^5)$ in the Galois field $GF(2^5)$.

---

*For a mathematical derivation of the syndrome registers, see Appendix III.

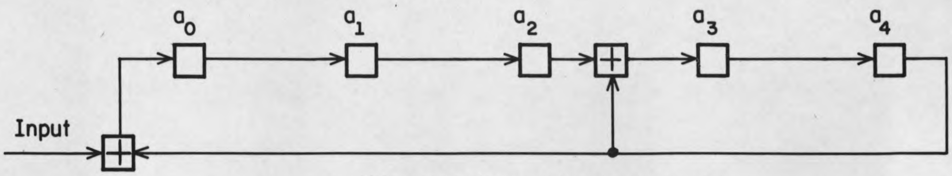


Figure 1a. Register S_1

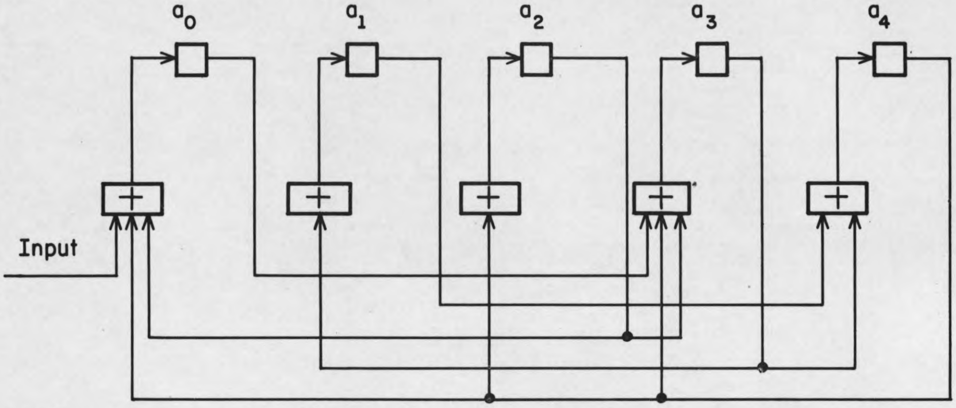


Figure 1b. Register S_3

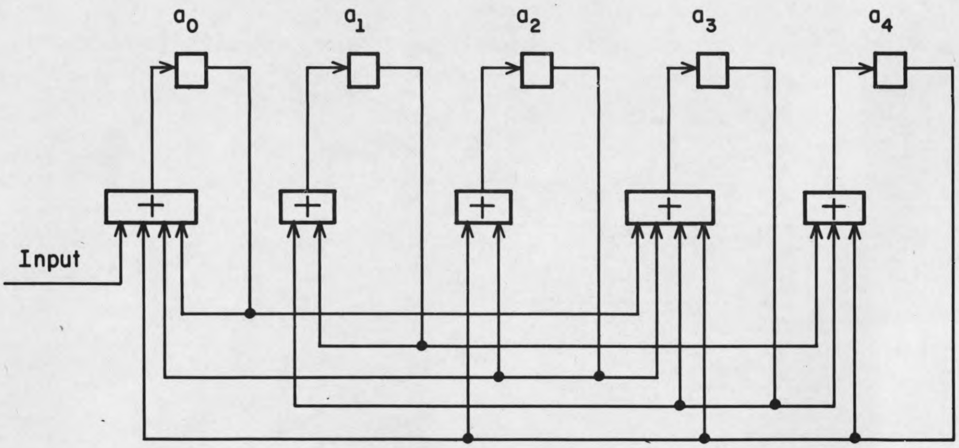


Figure 1c. Register S_5

⊞ Mod. 2 adder

☐ Storage element

Figure 1. Logical Schematics of Syndrome Registers

The two B functions are formed using the syndromes generated in the syndrome registers S_1, S_3, and S_5.

Since $B_1 = S_3[(S_1)^3 + S_3]$ and $B_2 = S_1[(S_1)^5 + S_5]$, two additional 5-stage Galois field shift registers modulo $(1 + x^3 + x^5)$ are needed to form, first, $(S_1)^3$ and $(S_1)^5$ respectively, and secondly, after the indicated polynomial additions in $GF(2^5)$ have been performed in accumulators AC_1 and AC_2, (see Figure 2) to perform the premultiplications by S_3 and S_1, respectively, with the results being placed into the accumulators AC_1 and AC_2. Countdowns and countups in $GF(2^5)$, which are necessary to control the shifts, are performed in countdown register A and countup register B (see Figure 3).

In addition to the equipment listed above, circuitry is needed to detect when all syndromes are zero, to keep track of the number of errors remaining in the code word, and to indicate when a trial correction is successful, i.e., when the error count has been reduced.

Operation of the Decoder (Brute Force Method)

The decoding procedure starts when the 32-bit code word has been received and loaded into the input buffer. We assume for purposes of discussion that bits x_0 to x_{15} are the 16 information bits, bits x_{16} to x_{30} are the BCH check bits, and x_{31} is the appended overall parity check bit. (The arrangement of the information bits within the code word may of course be varied to take advantage of certain statistical properties of error incidence.)

Initially, the overall parity check is computed, the syndromes S_1, S_3, and S_5 are generated and the B-functions are computed.

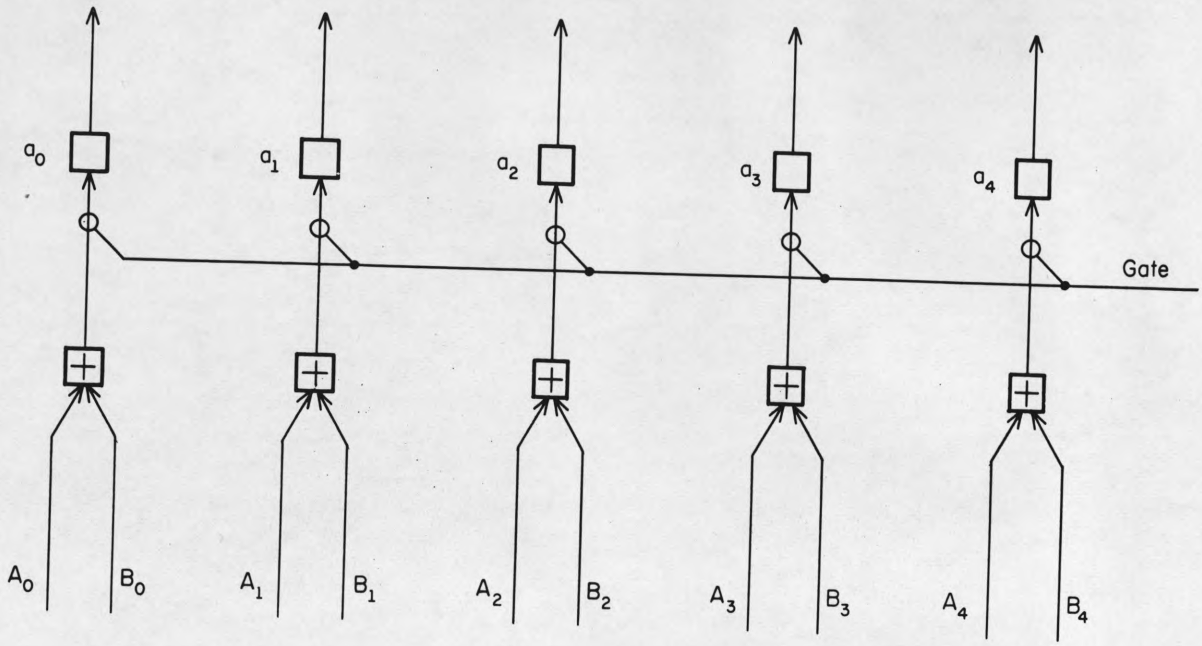


Figure 2. Galois Field (2^5) Adder Register

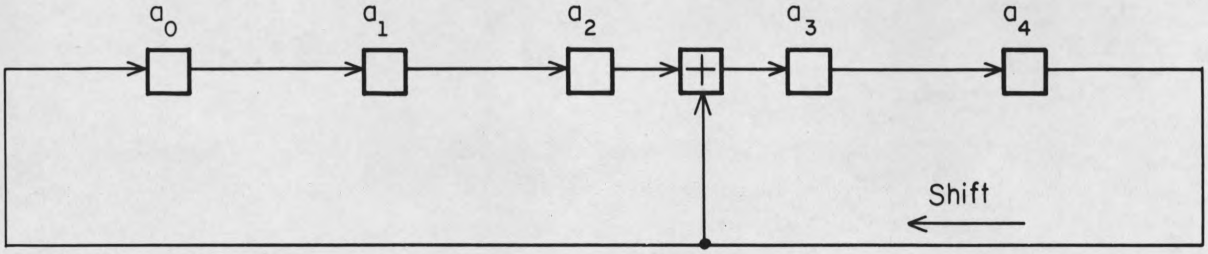


Figure 3a. Register B

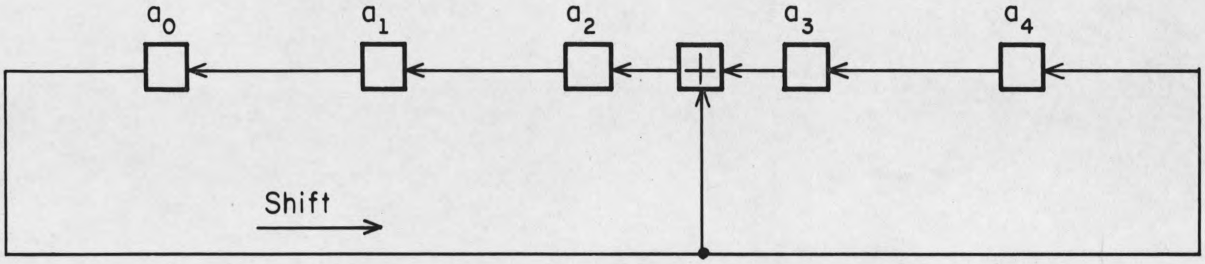


Figure 3b. Register A

Figure 3. Countup and Countdown Registers in GF(2^5)

a) If all syndromes are 0, then no error has occurred and the 16 information bits may be read out directly.

b) If $B_1 \neq B_2$ and the overall parity checks, then 4 errors have occurred during transmission. No correction is attempted under this condition, and an appropriate indication is given immediately. Note that the use of the overall parity check digit for the discrimination of 3 vs. 4 errors causes the case of 3 (correctable) errors in the code word plus a 4th error in the parity check digit to be classified as uncorrectable.

c) In all other cases, the initial error count indicated by B_1 and B_2 is remembered for later comparisons, and the sequential correction procedure is entered.

A cycle $i (i=0,1,2,...,30)$ in the iterative correction procedure consists of the following steps:

1. Perform a tentative correction at position i by complementing x_i.
2. Generate the syndromes S_1, S_3, and S_5 of the tentatively modified code word.
3. If all syndromes are now 0, all errors have been corrected. The remainder of the modified code word, i.e., digits x_i to x_{30}, may be read out directly.
4. If any syndrome is not 0, the functions B_1 and B_2 must be generated and the error count indicated by them compared with the previous error count.
5. If the number of errors was reduced by this tentative correction, then the complementation of x_i is accepted and the correct error count is updated; otherwise, x_i is recomplemented.
6. The digit x_i is now correct and may be read out.

7. The sequence of operations is repeated as cycle (i+1). The correction process terminates when all syndromes are 0 (step 3 above), which of course may not happen until the cycle for $i = 30$.

Improvements in the Method

a) Reduction to k Trial Correction Steps

Errors in the information digits are the only ones which must be corrected. Hence, regardless of the position of the information digits within the word, the correction procedure should be applied only to the k information digits, trapping whatever errors remain in the otherwise useless n-k check digits. Since $n = 2^m-1$ and $k = 2^{m-1}$, for the (31, 16), only about half the digits need be subjected to the correction phase. Of course, all errors may have been corrected in less than k cycles.

b) Elimination of Complete Regeneration of Syndromes in Each Correction Step

The generation of the syndromes, each of which is required not only initially but also in each recursive step of the correction procedure, requires 31 shifts. These shifts, during correction operations, can be eliminated in the following way:

1. An error in the r_0 position of the code word would have a syndrome of $\alpha^0 = 10000$ for S_1, S_3, S_5 if it were the only error present. Therefore, if there had been an error in the low-order position of the code word, we could add the syndrome for that error to S_1, S_3, S_5 and our detection circuit should indicate that the number of errors had decreased.

Remember that shifting right one place in S_1, S_3, S_5 is equivalent to multiplying them by α, α^3, α^5, mod $(1 + x^3 + x^5)$ in $GF(2^5)$ respectively. If we shift the code word and S_1, S_3, S_5 one place to the right, we may now add 10000 to the syndrome registers outputs and check our error count for the next bit in the sequence.

Utilizing this fact requires very little modification to our syndrome registers. We simply place mod 2 adders on the outputs adding 00000 for the initial error number count or 10000 during trial correction steps. This modification as applied to the S_1 register is shown in Figure 4 as an example. In addition, for every successful correction, 10000 is also added to S_1, S_3 and S_5 before shifting for the next cycle to correct the error in the syndrome registers.

The 31 cycle regeneration loop for calculation of S_1, S_3, S_5 in each trial correction has now been eliminated and we have gained a considerable increase in speed. Read-out is accomplished as correction is done as the code word is shifted to the right each trial.

Conclusions

We have developed and discussed a decoding procedure for BCH(n,k) codes under the constraints $m = 2^m - 1$, $d = 2t+1$, over Galois fields $GF(2^m)$ with $t \leq 3$. An error counting technique was employed as a means of judging results of a trial correction scheme rather than obtaining error locations by such methods are put forward by Chien*, Kasami**, Peterson***, et. al. The procedure proposed here seems to be independent of the redundancy of the code. We have developed a circuit for the BCH(32, 16) code which takes 16

---

*R. T. Chien, "Cyclic Decoding Procedures for Bose-Chaudhuri-Hocquenhem Codes," IEEE Trans. on Inf. Theory, IT-10, pp. 357-363 (1964).

**T. Kasami, "A Decoding Procedure for Multiple-Error-Correcting Cycle Codes," IEEE Trans. on Inf. Theory, IT-10, pp. 134-138 (1964).

***W. H. Peterson, "Encoding and Error-Correction Procedures for the Bose-Chaudhuri Codes," IRE Trans. on Inf. Theory, IT-6, pp. 459-470 (1960).

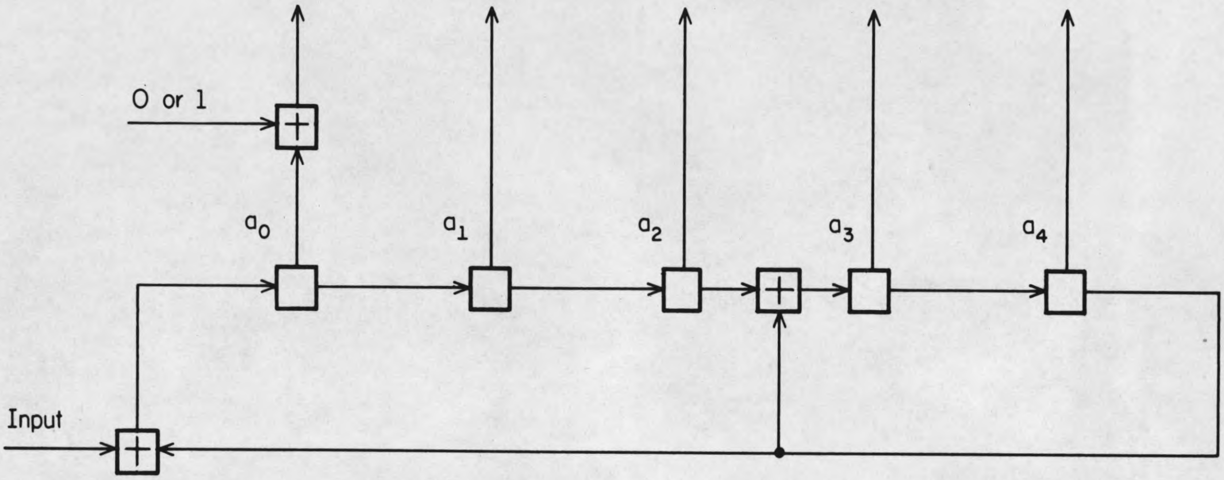


Figure 4. Tentative Correction Modification to Register S_1

correction cycles at the most to correct all acceptable errors in the information digits. As m of GF(2^m) becomes 6, 7, or 8 and the resulting codes expand, the ratio of r/n (r=n-k) decreases for the same value of t. By contrast, Kasami's procedure is dependent on high redundancy codes, the BCH (31, 11) code for example.

The big problem in implementation of the proposed decoding procedure is the error counting operation. No general theory is available at present for error counting in BCH codes. A logical layout of the error counting section of our hardware can be found in Figure 5. The "brute force" approach to the entire decoder system is laid out in Figure 6(a). The final configuration including our modifications is shown in Figure 6(b).

The Galois field arithmetic registers used in this procedure are rather simple in design. However, we paid for simplicity with time. For example, if we wished to multiply α^6 times α^{27}, we place α^{27} in register A and α^6 in register B. We then shift 28 times (until register A equals 10000). Then register B holds the result, α^3. The worst case time for a multiplication will occur when α^{30} is placed in register A to multiply any other α^i. However, as n grows large, the size of the registers involved is dependent only on the factor m of GF(2^m).

The ability to easily count the number of errors in a received code word removes the initial problem involved in Peterson's decoding procedure. In that procedure, the syndrome (power sums) matrix rank is dependent upon how many errors occurred. One way of solving this unknown factor is to assume t errors and find the determinant of M_T. If M_T is singular, try again for t-1 errors, and so on until M_T is non-singular. Massey* developed a procedure

---

*Massey, private communication to R. T. Chien.

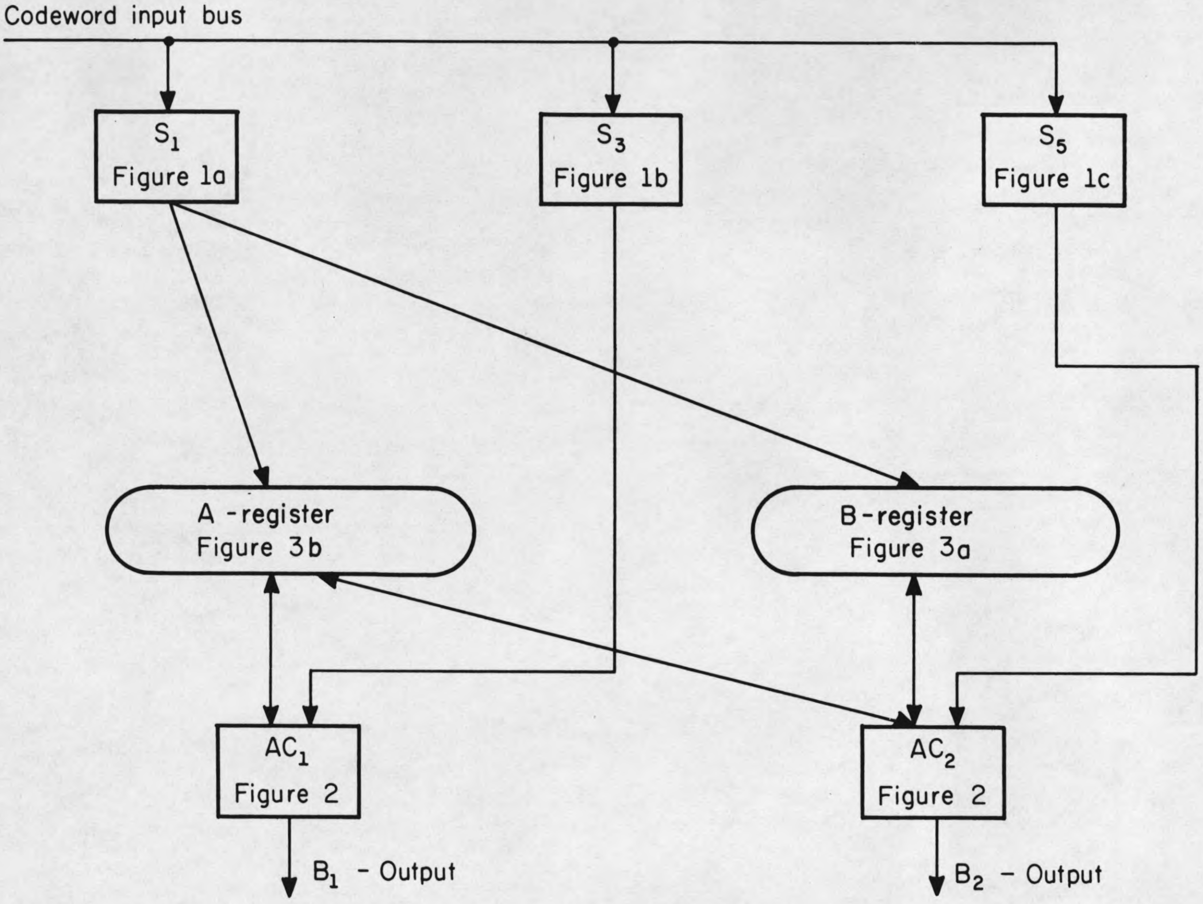


Figure 5. Error Counting Section Logical Layout

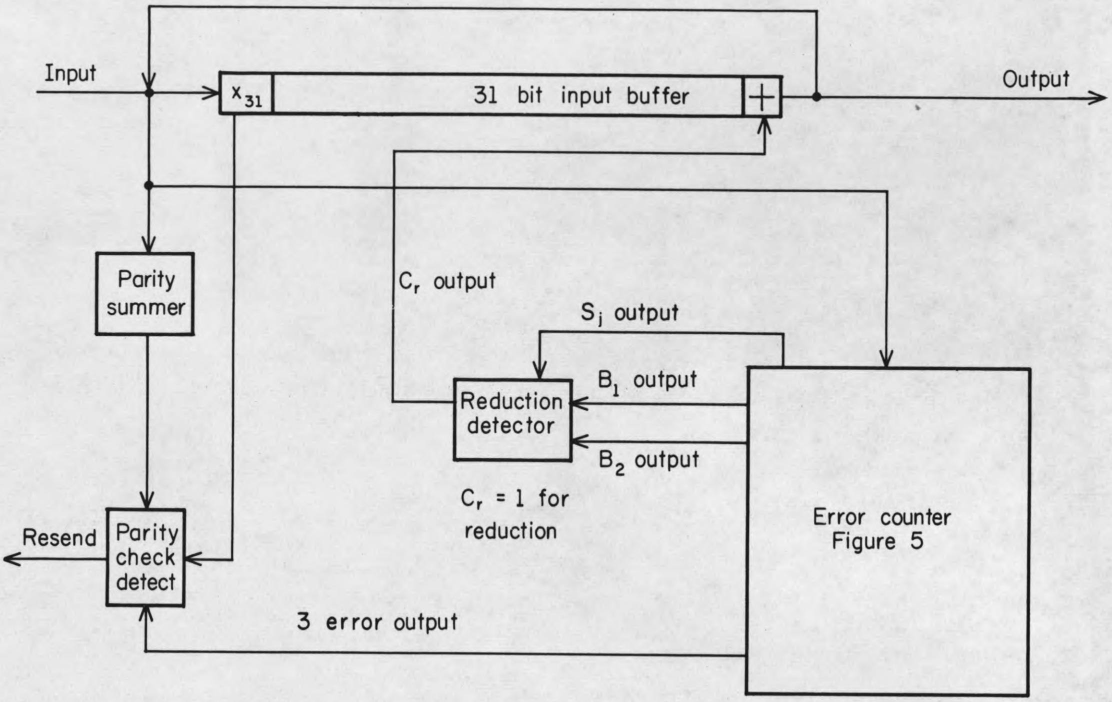


Figure 6a. Brute Force Configuration

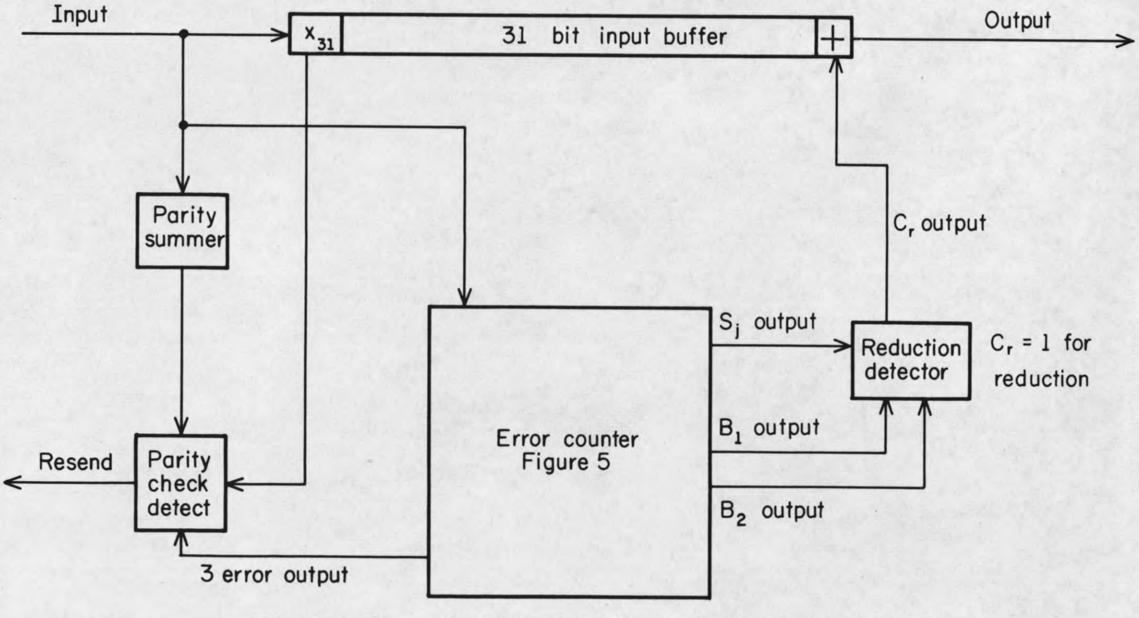


Figure 6b. Modified "Final" Configuration

Figure 6. Decoder System Logical Layouts

that is based on adding errors to the code word until M_T becomes non-singular. The proposed procedure does not rely on the non-singularity of M_T for solution and therefore is more powerful.

In our procedure, the time per correction step and hence the time for decoding one word varies according to the value of k for any BCH (n,k) code where k=n-mt. The position of the left-most error also influences the amount of decoding time by varying the number of correction cycles required.

Extension of this procedure to other BCH (n,k) codes where $t \leq 3$ is fairly straightforward. All $GF(2^5)$ field operating circuits are changed to $GF(2^m)$ and allowances for different operating times are made. A study must be made of the B_1 and B_2 functions to insure that $B_1 \neq B_2$ for 3 or 4 errors. Extending this problem to BCH codes with $t > 3$ will require the formulation of a suitable error counting scheme.

Appendix I

Kastenholz defines the functions B_1 and B_2 as:

$$B_1 = \frac{(S_1)^3 + S_3}{S_1} \qquad B_2 = \frac{(S_1)^5 + S_5}{S_3}$$

with the properties that:

for 1 error, S_1 is α^j

for 2 errors, S_1 is $\alpha^j + \alpha^{j+i}$

for 3 errors, S_1 is $\alpha^j + \alpha^{j+i} + \alpha^{j+k}$

for 4 errors, S_1 is $\alpha^j + \alpha^{j+i} + \alpha^{j+k} + \alpha^{j+h}$.

Actually, the B functions in general have the form

$$B_m = \frac{(S_1)^{2m+1} + S_{2m+1}}{S_{2m-1}}$$

Assume the existence of functions B_m and B_{m+n} $(m,n = 1,2,\ldots)$. For the one-error case, it can be easily seen that

$$B_m = B_{m+n} = 0 .$$

For the two-error cases,

$$B_m = \frac{(\alpha^j + \alpha^{j+i})\ (\alpha^{pj} + \alpha^{pj+pi}) + \alpha^{rj} + \alpha^{rj+ri}}{\alpha^{nj} + \alpha^{nj+ni}}$$

where $n = 2m-1$

$p = 2m$

$r = 2m+1$

$$B_m = \frac{\alpha^{rj+i} + \alpha^{rj+pi}}{\alpha^{nj}\ (\alpha^0 + \alpha^{ni})}$$

$$= \frac{\alpha^{rj}\ (\alpha^{i} + \alpha^{pi})}{\alpha^{nj}\ (\alpha^{0} + \alpha^{ni})}$$

$$= \alpha^{(r-n)j}\ \frac{(\alpha^{i}\ (\alpha^{0} + \alpha^{(p-1)i})}{\alpha^{0} + \alpha^{ni}}$$

Now $n = p-1$, and $r-n = 2$. Then B_m reduces to $B_m = \alpha^{2j+i}$. For the three-error case, the syndromes result from

$$\alpha^{j} + \alpha^{j+i} + \alpha^{j+k}$$

Formulating B_m and B_{m+n} and setting them equal to each other, we find (after some manipulation):

$$\begin{aligned}
&\alpha^{(2m-1)i} + \alpha^{(2m-1)k} + \alpha^{(2m-2)i} + \alpha^{(2m-2)k} \\
&\quad + \alpha^{(2m+2n-1)i + (2m-2)k} + \alpha^{(2m-2)i + (2m+2n-1)k} \\
&\quad + \alpha^{(2m-2n-2)i + (2m-2)k} + \alpha^{(2m-2)i + (2m+2n-2)k} \\
&\quad = 0 .
\end{aligned}$$

Inspection shows that the above equation will be zero only in the case where $i = k$. But in the three-error case, $i \neq 0$, $k \neq 0$ and $i \neq k$. So $B_m \neq B_{m+n}$.

For the final proof of the validity of the procedure, we need to look at the function $B_1 + B_2$ in the case of four-errors.

The formulas for B_1 and B_2 now become the following:

$$B_1 = \frac{(\alpha^{j} + \alpha^{j+i} + \alpha^{j+k} + \alpha^{j+h})\ (\alpha^{2j} + \alpha^{2(j+i)} + \alpha^{2(j+k)} + \alpha^{2(j+h)})}{D_3}$$

$$+ \frac{\alpha^{3j} + \alpha^{3(j+i)} + \alpha^{3(j+k)} + \alpha^{3(j+h)}}{D_3}$$

$$B_2 = \frac{(\alpha^{i} + \alpha^{j+i} + \alpha^{j+k} + \alpha^{j+h})(\alpha^{4j} + \alpha^{4(j+i)} + \alpha^{4(j+k)} + \alpha^{4(j+h)})}{D_1}$$

$$+ \frac{\alpha^{5j} + \alpha^{5(j+i)} + \alpha^{5(j+k)} + \alpha^{5(j+h)}}{D_1}$$

where

$$D_1 = \alpha^{j} + \alpha^{j+i} + \alpha^{j+k} + \alpha^{j+h}$$

and

$$D_3 = \alpha^{3j} + \alpha^{3(j+i)} + \alpha^{3(j+k)} + \alpha^{3(j+h)}$$

A Fortran 60 program was written on the CDC 1604 to evaluate the function $B_1 + B_2$ for all possible permissible values of i, k, and h. The constraints on i, k, and h are the following:

$$i \neq k \neq h \neq 0$$

The values of i, k, and h ran over the following ranges:

i from 1 to 30

k from i+1 to 30

h from k+1 to 30

It is obvious that these ranges satisfy the constraints on i, k, and h. In addition, the program checked only one of each type (i.e., the case $i = 1$, $k = 2$, and $h = 3$, but not also $i = 1$, $k = 3$, and $h = 2$ as the results are the same). Let us remember that this proof by perfect induction was applied only to the case of the $GF(2^5)$ field.

The number of possible combinations for $n = 30$ is

$$N_C = \frac{30!}{3!\ 27!} = 4060$$

No zeros of $B_1 + B_2$ were found in the 4060 possible cases.

In performing this test of the functions B_1 and B_2, we were mainly interested in showing that $B_1 \neq B_2$ in all permissible four-error cases. We must remind the reader that this was done only for the (31, 16) code over $GF(2^5)$. There is an interesting problem here for research by some other party in trying to find the theory behind the behavior of the B_1 and B_2 functions for (n,k) codes over $GF(2^m)$.

Appendix II

We develop here the BCH (31, 16) code used in this paper. We are interested in obtaining the h(x) polynomial for the construction of the encoder.

Recall that the BCH codes are generated by the polynomial, g(x), which has roots

$$\alpha^{m_0}, \alpha^{m_0+1}, \alpha^{m_0+2}, \ldots, \alpha^{m_0+d-2}$$

where α is the primitive element of a field $GF(2^m)$, and d is the minimum Hamming distance between any two code points in the code space.

Using Peterson's notation[*], we set $m_0 = 1$, select α as the primitive element of the field $GF(2^5)$ mod $(\alpha^5 + \alpha^3 + 1)$ and choose $d = 2t + 1 = 7 (t=3)$. Then, $\alpha, \alpha^3, \ldots, \alpha^{2t-1}$ are roots of our code vector $\{f(x)\}$. If $m_i(x)$ denotes the minimum function of α^i, then

$$g(x) = LCM(m_1(x), m_3(x), \ldots, m_{2t-1}(x))$$

For t = 3

$$g(x) = m_1(x)\ m_3(x)\ m_5(x)$$

The minimum functions are all of degree 5.

We can easily see that the roots of the three minimum functions are as follows:

$\alpha^1\ \alpha^2\ \alpha^4\ \alpha^8\ \alpha^{16}$	$m_1(x)$
$\alpha^3\ \alpha^6\ \alpha^{12}\ \alpha^{24}\ \alpha^{17}$	$m_3(x)$
$\alpha^5\ \alpha^{10}\ \alpha^{20}\ \alpha^9\ \alpha^{18}$	$m_5(x)$

We extract the minimum functions from the following equations.

---

[*] Peterson, W. W., Error Correcting Codes, MIT Press, Cambridge, Mass., pp. 164-167 (1961).

$$m_1(x) = (X - \alpha)\ (X - \alpha^2)\ (X - \alpha^4)\ (X - \alpha^8)\ (X - \alpha^{16})$$

$$m_3(x) + (X - \alpha^3)\ (X - \alpha^6)\ (X - \alpha^{12})\ (X - \alpha^{24})\ (X - \alpha^{17})$$

$$m_5(x) = (X - \alpha^5)\ (X - \alpha^{10})\ (X - \alpha^{20})\ (X - \alpha^9)\ (X - \alpha^{18})$$

Table I gives the appropriate polynomial configurations for the α^i's. With some mathematical manipulation we arrive at the following minimum functions:

$$m_1(x) = 1 + X^3 + X^5$$

$$m_3(x) = 1 + X + X^2 + X^3 + X^5$$

$$m_5(x) = 1 + X + X^3 + X^4 + X^5$$

More manipulation leads to

$$g(x) = 1 + X^4 + X^5 + X^6 + X^7 + X^8 + X^{10} + X^{12} + X^{13} + X^{14} + X^{15}$$

H(x) is given by the formula $h(x) = \dfrac{X^{31} + 1}{g(x)}$

After much long division laboring, we obtain

$$h(x) = X^{16} + X^{15} + X^{12} + X^7 + X^6 + X^5 + X^4 + 1$$

The encoding scheme used in the computer simulation of this procedure is described by Peterson* as a k stage encoder with connections based upon

$$h(x) = x^n - 1/g(x)$$

Figure 7 shows the logical configuration of the encoder.

---

*Op. cit., page 148.

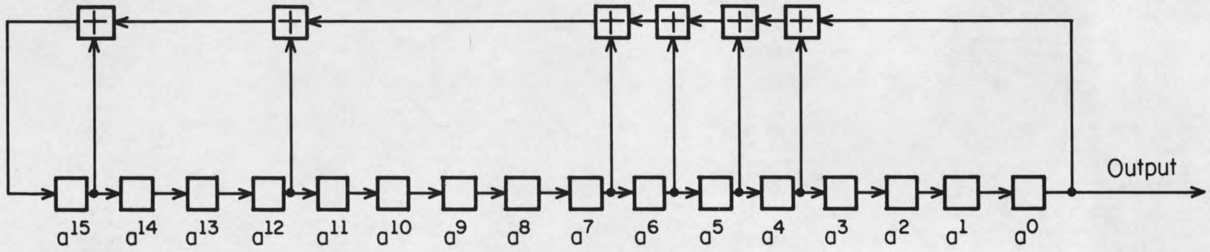


Figure 7. Encoder Register for BCH(31,16) Code

Appendix III

Since the received vector is $r(x)$, $r(x) = c(x) + e(x)$ where $e(x)$ is the error vector, $c(x)$ is divisible by $g(x)$ and $c(x)\, H^T = 0$. Therefore, we are left with

$$r(x) H^T = e(x)\, H^T = (S_1\ S_3\ S_5)$$

Since $m = 5$ and $n = 2^m - 1 = 31$, we are operating in a field $GF(2^5)$ with 32 elements.

The primitive polynomial of degree 5 is

$$K(x) = 1 + x^3 + x^5 \quad \text{or} \quad x^5 = 1 + x^3$$

There are 32 code words corresponding to

$$\alpha^j (0 \leq j \leq 30);\ \alpha^{31} = \alpha^0 = 1$$

and of course

00000

Table I lists all of the powers of α.

A Galois field shift register for $\alpha^5 = \alpha^3 + 1$ is the circuit shown in Figure 1(a).

For the S_3 syndrome, we multiply by α^3

$$1 \cdot \alpha^3 = \alpha^3$$

$$\alpha \cdot \alpha^3 = \alpha^4$$

$$\alpha^2 \cdot \alpha^3 = \alpha^5 = 1 + \alpha^3$$

$$\alpha^3 \cdot \alpha^3 = \alpha^6 = \alpha + \alpha^4$$

$$\alpha^4 \cdot \alpha^3 = \alpha^7 = 1 + \alpha^2 + \alpha^3$$

We determine our new values of a_0, a_1, a_2, a_3, and a_4 as follows:

$$\alpha^3 (a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4)$$

$$= a_0\alpha^3 + a_1\alpha^4 + a_2(1 + \alpha^3)$$

$$+ a_3(\alpha + \alpha^4) + a_4(1 + \alpha^2 + \alpha^3)$$

$$= a_0\alpha^3 + a_1\alpha^4 + a_2 + a_2\alpha^3$$

$$+ a_3\alpha + a_3\alpha^4 + a_4 + a_4\alpha^2 + a_4\alpha^3$$

$$= (a_2 + a_4) + \alpha(a_3)$$

$$+ \alpha^2(a_4) + \alpha^3(a_0 + a_2 + a_4)$$

$$+ \alpha^4(a_1 + a_3)$$

So our old values of a_i are converted as:

$$\alpha^3$$

$$a_0 \longrightarrow a_2 + a_4$$

$$a_1 \longrightarrow a_3$$

$$a_2 \longrightarrow a_4$$

$$a_3 \longrightarrow a_0 + a_2 + a_4$$

$$a_4 \longrightarrow a_1 + a_3$$

Now we develop a shift register as shown in Figure 1(b).

For the S_5 syndrome, we must design a circuit from the following equations. Multiplying by α^5 gives:

$$1 \cdot \alpha^5 = 1 + \alpha^3$$

$$\alpha \cdot \alpha^5 = \alpha^6 = \alpha + \alpha^4$$

$$\alpha^2 \cdot \alpha^5 = \alpha^7 = 1 + \alpha^2 + \alpha^3$$

$$\alpha^3 \cdot \alpha^5 = \alpha^8 = \alpha + \alpha^3 + \alpha^4$$

$$\alpha^4 \cdot \alpha^5 = \alpha^9 = 1 + \alpha^2 + \alpha^3 + \alpha^4$$

Again, we determine new values for a_0, a_1, a_2, a_3, and a_4:

$$\alpha^5(a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4)$$

$$= \alpha^5 a_0 + a_1\alpha^6 + a_2\alpha^7 + a_3\alpha^8 + a_4\alpha^9$$

$$= a_0(1+\alpha^3) + a_1(\alpha + \alpha^4)$$

$$+ a_2(1 + \alpha^2 + \alpha^3)$$

$$+ a_3(\alpha + \alpha^3 + \alpha^4)$$

$$+ a_4(1 + \alpha^2 + \alpha^3 + \alpha^4)$$

Now collecting terms:

$$= (a_0 + a_2 + a_4)$$

$$+ (a_1 + a_3)\alpha$$

$$+ (a_2 + a_4)\alpha^2$$

$$+ (a_0 + a_2 + a_3 + a_4)\alpha^3$$

$$+ (a_1 + a_3 + a_4)\alpha^4$$

The old values of the a_i's are converted as follows:

a^5

$a_0 \longrightarrow (a_0 + a_2 + a_4)$

$a_1 \longrightarrow (a_1 + a_3)$

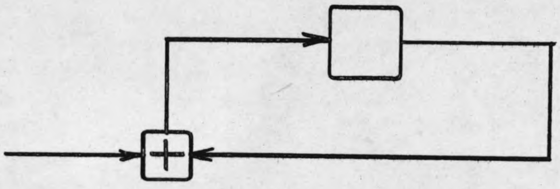
$a_2 \longrightarrow (a_2 + a_4)$

$a_3 \longrightarrow (a_0 + a_2 + a_3 + a_4)$

$a_4 \longrightarrow (a_1 + a_3 + a_4)$

The circuit follows as in Figure 1(c).

For the checking of parity for comparison with x_{31}, we use the following simple circuit.



Circuit for Summing 1's Digits in a Code Word

Figure 8

Acknowledgement

The author is indebted to Dr. Robert T. Chien of the Coordinated Science Laboratory at the University of Illinois for his very helpful instruction in coding theory. Also, acknowledgment is made of the many helpful suggestions made by Dr. Gernot Metze, also of the Coordinated Science Laboratory, during preparation of this paper.

TABLE I

Representation of GF(2^5)

$\alpha^{0} = 1 = (10000)$
$\alpha^{1} = \alpha = (01000)$
$\alpha^{2} = \alpha^{2} = (00100)$
$\alpha^{3} = \alpha^{3} = (00010)$
$\alpha^{4} = \alpha^{4} = (00001)$
$\alpha^{5} = 1 + \alpha^{3} = (10010)$
$\alpha^{6} = \alpha + \alpha^{4} = (01001)$
$\alpha^{7} = 1 + \alpha^{2} + \alpha^{3} = (10110)$
$\alpha^{8} = \alpha + \alpha^{3} + \alpha^{4} = (01011)$
$\alpha^{9} = 1 + \alpha^{2} + \alpha^{3} + \alpha^{4} = (10111)$
$\alpha^{10} = 1 + \alpha + \alpha^{4} = (11001)$
$\alpha^{11} = 1 + \alpha + \alpha^{2} + \alpha^{3} = (11110)$
$\alpha^{12} = \alpha + \alpha^{2} + \alpha^{3} + \alpha^{4} = (01111)$
$\alpha^{13} = 1 + \alpha^{2} + \alpha^{4} = (10101)$
$\alpha^{14} = 1 + \alpha = (11000)$
$\alpha^{15} = \alpha + \alpha^{2} = (01100)$
$\alpha^{16} = \alpha^{2} + \alpha^{3} = (00110)$
$\alpha^{17} = \alpha^{3} + \alpha^{4} = (00011)$
$\alpha^{18} = 1 + \alpha^{3} + \alpha^{4} = (10011)$
$\alpha^{19} = 1 + \alpha + \alpha^{3} + \alpha^{4} = (11011)$
$\alpha^{20} = 1 + \alpha + \alpha^{2} + \alpha^{2} + \alpha^{4} = (11111)$
$\alpha^{21} = 1 + \alpha + \alpha^{2} + \alpha^{4} = (11101)$
$\alpha^{22} = 1 + \alpha + \alpha^{2} = (11100)$
$\alpha^{23} = \alpha + \alpha^{2} + \alpha^{3} = (01110)$
$\alpha^{24} = \alpha^{2} + \alpha^{3} + \alpha^{4} = (00111)$
$\alpha^{25} = 1 + \alpha^{4} = (10001)$
$\alpha^{26} = 1 + \alpha + \alpha^{3} = (11010)$
$\alpha^{27} = \alpha + \alpha^{2} + \alpha^{4} = (01101)$
$\alpha^{28} = 1 + \alpha^{2} = (10100)$
$\alpha^{29} = \alpha + \alpha^{3} = (01010)$
$\alpha^{30} = \alpha^{2} + \alpha^{4} = (00101)$
$\alpha^{31} = \alpha^{0} = 1$

Distribution list as of March 1, 1965

1 Dr. Chalmers Sherwin
Deputy Director (Research & Technology)
DD&RE Rm 3E1060
The Pentagon
Washington, D. C. 20301

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res & Eng
Department of Defense
Washington, D. C. 20301

1 Dr. James A. Ward
Office of Deputy Director (Research and
Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Mr. Charles Yost, Director
for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

20 Defense Documentation Center
Cameron Station, Bldg. 5
Alexandria, Virginia 22314
Attn: TISIA

1 Director
National Security Agency
Fort George G. Meade, Maryland 20755
Attn: Librarian C-332

1 Chief of Research and Development
Headquarters, Department of the Army
Washington, D. C. 20310
Attn: Physical Sciences Division P & E

1 Chief of Research and Development
Headquarters, Department of the Army
Washington, D. C. 20310
Attn: Mr. L. H. Geiger, Rm 34442

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications
Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: V. W. Richards

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: Keats A. Pullen, Jr.

1 Commanding Officer
U. S. Army Ballistics Research Lab.
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: George C. Francis, Computing Lab.

1 Commandant
U. S. Army Air Defense School
P. O. Box 9390
Fort Bliss, Texas 79916
Attn: Missile Sciences Div., C&S Dept.

1 Commanding General
U. S. Army Missile Command
Redstone Arsenal, Alabama 35809
Attn: Technical Library

1 Commanding General
Frankford Arsenal
Philadelphia, Pa. 19137
Attn: SMUFA-1310 (Dr. Sidney Ross)

1 Commanding General
Frankford Arsenal
Philadelphia, Pa. 19137
Attn: SMUFA-1300

1 U. S. Army Munitions Command
Picatinney Arsenal
Dover, New Jersey 07801
Attn: Technical Information Branch

1 Commanding Officer
Harry Diamond Laboratories
Connecticut Ave. & Van Ness St., N.W.
Washington, D. C. 20438
Attn: Mr. Berthold Altman

1 Commanding Officer
Harry Diamond Laboratories
Attn: Library
Connecticut Ave. & Van Ness St., N.W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Aberdeen Proving Ground
Aberdeen, Maryland 21005
Attn: Technical Director

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army EngineerGeodesy. Intelligence
and Mapping, Research & Devel. Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General
Staff College
Fort Leavenworth, Kansas 66207
Attn: Secretary

1 Dr. H. Robl, Deputy Director
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
P. O. Box CM, Duke Station
Durham, North Carolina 27706
Attn: CRD-AA-IP (Richard O. Ulsh)

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703
Attn: AMSEL-SC

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: Dr. S. Benedict Levin, Director
Institute for Exploratory Research

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: Mr. Robert O. Parker, Executive
Secretary, JSTAC (AMSEL-RD-X)

1 Superintendent
U. S. Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Army Medical Center
Washington, D. C. 20012

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-DR

1 Director
U. S. Army Electronics Laboratories
Attn: AMSEL-RD-X
Fort Monmouth, New Jersey 07703

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XC

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-XS

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NO

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-NP

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SA

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-SS

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PE

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PF

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-PR

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RL-GF

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-ADT

1 Director
U. S. Army Electronics Laboratories
Fort Monmouth, New Jersey 07703
Attn: AMSEL-RD-FU#1

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineers R&D Laboratory
Fort Belvoir, Virginia 22060
Attn: STINFO Branch

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range
New Mexico 88002

1 Director
Human Resources Research Office
The George Washington University
300 N. Washington Street
Alexandria, Virginia

1 Commanding Officer
U. S. Army Personnel Research Office
Washington 25, D. C.

1 Commanding Officer
U. S. Army Medical Research Laboratory
Fort Knox, Kentucky

1 Commanding General
U. S. Army Signal Center and School
Attn: Chief, Office of Academic
Operations
Fort Monmouth, New Jersey 07703

2 Dr. Richard H. Wilcox, Code 437
Department of the Navy
Washington, D. C. 20360

1 Chief, Bureau of Weapons
Attn: Technical Library, DL1-3
Department of the Navy
Washington, D. C. 20360

1 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360
Attn: Code 680

1 Chief, Bureau of Ships
Department of the Navy
Washington, D. C. 20360
Attn: Code 732

1 Commander
U. S. Naval Air Development Center
Johnsville, Pennsylvania
Attn: NADC Library

1 Commanding Officer
Naval Electronics Laboratory
San Diego, California 92052
Attn: Code 2222(Library)

1 Commanding Officer
Naval Electronics Laboratory
San Diego, California 92052
Attn: Code 2800, C. S. Manning

1 Commanding Officer and Director
(Code 142 Library)
David W. Taylor Model Basin
Washington, D. C. 20007

6 Director
Naval Research Laboratory
Washington, D. C. 20390
Attn: Technical Information Office
(Code 2000)

1 Commanding Officer
Office of Naval Research Branch Office
219 S. Dearborn Street
Chicago, Illinois 60604

1 Chief of Naval Operations
Department of the Navy
Washington, D. C. 20350
Attn: OP-07T

1 Chief of Naval Operations
Department of the Navy
Washington, D. C. 20350
Attn: OP-03EG

1 Commanding Officer
Office of Naval Research Branch Office
1000 Geary Street
San Francisco, California 94109

1 Commanding Officer
U. S. Naval Weapons Laboratory
Asst. Director for Computation
Dahlgren, Virginia 22448
Attn: G. H. Gleissner (Code K-4)

1 Inspector of Naval Material
Bureau of Ships Technical Representative
1902 West Minnehaha Avenue
St. Paul 4, Minnesota

5 Lt. Col. E. T. Gaines, SREE
Chief, Electronics Division
Directorate of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 Director of Science & Technology
Deputy Chief of Staff (R & D)
USAF
Washington, D. C.
Attn: AFRST-EL/GU

1 Director of Science & Technology
Deputy Chief of Staff (R & D)
USAF
Washington, D. C.
Attn: AFRST-SC

1 Karl M. Fuechsel
Electronics Division
Director of Engineering Sciences
Air Force Office of Scientific Research
Washington, D. C. 20333

1 Lt. Col. Edwin M. Myers
Headquarters, USAF (AFRDR)
Washington 25, D. C.

1 Director, Air University Library
Maxwell Air Force Base
Alabama 36112
Attn: CR-4803a

1 Commander
Research & Technology Division
AFSC (Mr. Robert L. Feik)
Office of the Scientific Director
Bolling AFB 25, D. C.

1 Commander
Research & Technology Division
Office of the Scientific Director
Bolling AFB 25, D. C.
Attn: RTHR

1 Commander
Air Force Cambridge Research Laboratories
Attn: Research Library
CRMXL-R
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Dr. Lloyd Hollingsworth
AFCRL
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Commander
Air Force Cambridge Research Laboratories
Attn: Data Sciences Lab
(Lt. S. J. Kahne, CRB)
L. G. Hanscom Field
Bedford, Massachusetts 01731

1 Commander
Air Force Systems Command
Office of the Chief Scientist
(Mr. A. G. Wimer)
Andrews AFB, Maryland 20331

1 Commander
Air Force Missile Development Center
Attn: MDSGO/Major Harold Wheeler, Jr.
Holloman Air Force Base, New Mexico

1 Commander
Research & Technology Division
Attn: MAYT (Mr. Evans)
Wright-Patterson Air Force Base
Ohio 45433

1 Directorate of Systems Dynamics Analysis
Aeronautical Systems Division
Wright-Patterson AFB, Ohio 45433

1 Hqs. Aeronautical Systems Division
AF Systems Command
Attn: Navigation & Guidance Laboratory
Wright-Patterson AFB, Ohio 45433

1 Commander
Rome Air Development Center
Attn: Documents Library, RAALD
Griffiss Air Force Base
Rome, New York 13442

1 Commander
Rome Air Development Center
Attn: RAWI-Major W. H. Harris
Griffiss Air Force Base
Rome, New York 13442

1 Lincoln Laboratory
Massachusetts Institute of Technology
P. O. Box 73
Lexington 73, Massachusetts
Attn: Library A-082

Continued next page

Distribution list as of March 1, 1965 (Cont'd.)

1 Lincoln Laboratory
Massachusetts Institute of Technology
P. O. Box 73
Lexington 73, Massachusetts
Attn: Dr. Robert Kingston

1 APGC (PGAPI)
Eglin Air Force Base
Florida

1 Mr. Alan Barnum
Rome Air Development Center
Griffiss Air Force Base
Rome, New York 13442

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61803

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California

1 Director
Electronics Research Laboratory
University of California
Berkeley 4, California

1 Professor A. A. Dougal, Director
Laboratories for Electronics and Related
Science Research
University of Texas
Austin, Texas 78712

1 Professor J. K. Aggarwal
Department of Electrical Engineering
University of Texas
Austin, Texas 78712

1 Director of Engineering & Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

1 Capt. Paul Johnson (USN Ret.)
National Aeronautics & Space Agency
1520 H. Street, N. W.
Washington 25, D. C.

1 NASA Headquarters
Office of Applications
400 Maryland Avenue, S.Q.
Washington 25, D. C.
Attn: Code FC Mr. A. M. Greg Andrus

1 National Bureau of Standards
Research Information Center and Advisory
Serv. on Info. Processing
Data Processing Systems Division
Washington 25, D. C.

1 Dr. Wallace Sinaiko
Institute for Defense Analyses
Research & Eng. Support Div.
1666 Connecticut Avenue, N. W.
Washington 9, D. C.

1 Data Processing Systems Division
National Bureau of Standards
Conn. at Van Ness
Room 239, Bldg. 10
Washington 25, D. C.
Attn: A. K. Smilow

1 Exchange and Gift Division
The Library of Congress
Washington 25, D. C.

1 Dr. Alan T. Waterman, Director
National Science Foundation
Washington 25, D. C.

1 H. E. Cochran
Oak Ridge National Laboratory
P. O. Box X
Oak Ridge, Tennessee

1 U. S. Atomic Energy Commission
Office of Technical Information Extension
P. O. Box 62
Oak Ridge, Tennessee

1 Mr. G. D. Watson
Defense Research Member
Canadian Joint Staff
2450 Massachusetts Avenue, N. W.
Washington 8, D. C.

1 Martin Company
P. O. Box 5837
Orlando, Florida
Attn: Engineering Library MP-30

1 Laboratories for Applied Sciences
University of Chicago
6220 South Drexel
Chicago, Illinois 60637

1 Librarian
School of Electrical Engineering
Purdue University
Lafayette, Indiana

1 Donald L. Epley
Dept. of Electrical Engineering
State University of Iowa
Iowa City, Iowa

1 Instrumentation Laboratory
Massachusetts Institute of Technology
68 Albany Street
Cambridge 39, Massachusetts
Attn: Library WI-109

1 Sylvania Electric Products, Inc.
Electronics System
Waltham Labs. Library
100 First Avenue
Waltham 54, Massachusetts

2 Hughes Aircraft Company
Centinela and Teale Streets
Culver City, California
Attn: K. C. Rosenberg, Supervisor
Company Technical Document Center

3 Autonetics
9150 East Imperial Highway
Downey, California
Attn: Tech. Library, 3041-11

1 Dr. Arnold T. Nordsieck
General Motors Corporation
Defense Research Laboratories
6767 Hollister Avenue
Goleta, California

1 University of California
Lawrence Radiation Laboratory
P. O. Box 808
Livermore, California

1 Mr. Thomas L. Hartwick
Aerospace Corporation
P. O. Box 95085
Los Angeles 45, California

1 Lt. Col. Willard Levin
Aerospace Corporation
P. O. Box 95085
Los Angeles 45, California

1 Sylvania Electronic Systems-West
Electronic Defense Laboratories
P. O. Box 205
Mountain View, California
Attn: Documents Center

1 Varian Associates
611 Hansen Way
Palo Alto, California 94303
Attn: Tech. Library

1 Huston Denslow
Library Supervisor
Jet Propulsion Laboratory
California Institute of Technology
Pasadena, California

1 Professor Nicholas George
California Institute of Technology
Electrical Engineering Department
Pasadena, California

1 Space Technology Labs., Inc.
One Space Park
Redondo Beach, California
Attn: Acquisitions Group
STL Technical Library

1 The Rand Corporation
1700 Main Street
Santa Monica, California
Attn: Library

1 Miss F. Cloak
Radio Corp. of America
RCA Laboratories
David Sarnoff Research Center
Princeton, New Jersey

1 Mr. A. A. Lundstrom
Bell Telephone Laboratories
Room 2E-127
Whippany Road
Whippany, New Jersey

1 Cornell Aeronautical Laboratory, Inc.
4455 Genesee Street
Buffalo 21, New York
Attn: J. P. Desmond, Librarian

1 Sperry Gyroscope Company
Marine Division Library
155 Glenn Cove Road
Carle Place, L. I., New York
Attn: Miss Barbara Judd

1 Library
Light Military Electronics Dept.
General Electric Company
Armament & Control Products Section
Johnson City, New York

1 Dr. E. Howard Holt
Director
Plasma Research Laboratory
Rennselaer Polytechnic Institute
Troy, New York

1 Battele-DEFENDER
Battelle Memorial Institute
505 King Avenue
Columbus 1, Ohio

1 Laboratory for Electroscience Research
New York University
University Heights
Bronx 53, New York

1 National Physical Laboratory
Teddington, Middlesex
England
Attn: Dr. A. M. Uttley, Superintendent,
Autonomics Division

1 Dr. Lee Huff
Behavioral Sciences
Advanced Research Projects Agency
The Pentagon (Room 3E175)
Washington, D. C. 20301

1 Dr. Glenn L. Bryan
Head, Personnel and Training Branch
Office of Naval Research
Navy Department
Washington, D. C. 20360

1 Instituto de Fisica Aplicado
"L. Torres Quevedo"
High Vacuum Laboratory
Madrid, Spain
Attn: Jose L. de Segovia

1 Stanford Research Institute
Attn: G-037 External Reports
(for J. Goldberg)
Menlo Park, California 94025

REVISED U. S. ARMY DISTRIBUTION LIST

(As received at the Coordinated Science Laboratory 27 July 1965)

1 Dr. Chalmers Sherwin
Deputy Director (Research & Technology)
DD&RE Rm 3E1060
The Pentagon
Washington, D. C. 20301

1 Dr. Edward M. Reilley
Asst. Director (Research)
Ofc. of Defense Res. & Eng.
Department of Defense
Washington, D. C. 20301

1 Dr. James A. Ward
Office of Deputy Director (Research
and Information Rm 3D1037)
Department of Defense
The Pentagon
Washington, D. C. 20301

1 Director
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Mr. E. I. Salkovitz, Director
for Materials Sciences
Advanced Research Projects Agency
Department of Defense
Washington, D. C. 20301

1 Colonel Charles C. Mack
Headquarters
Defense Communications Agency (333)
The Pentagon
Washington, D. C. 20305

20 Defense Documentation Center
Attn: TISIA
Cameron Station, Building 5
Alexandria, Virginia 22314

1 Director
National Security Agency
Attn: Librarian C-332
Fort George G. Meade, Maryland 20755

1 U. S. Army Research Office
Attn: Physical Sciences Division
3045 Columbia Pike
Arlington, Virginia 22204

1 Chief of Research and Development
Headquarters, Department of the Army
Attn: Mr. L. H. Geiger, Rm 3D442
Washington, D. C. 20310

1 Research Plans Office
U. S. Army Research Office
3045 Columbia Pike
Arlington, Virginia 22204

1 Commanding General
U. S. Army Materiel Command
Attn: AMCRD-RS-PE-E
Washington, D. C. 20315

1 Commanding General
U. S. Army Strategic Communications Command
Washington, D. C. 20315

1 Commanding Officer
U. S. Army Materials Research Agency
Watertown Arsenal
Watertown, Massachusetts 02172

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: V. W. Richards
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: Keats A. Pullen, Jr.
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
U. S. Army Ballistics Research Laboratory
Attn: George C. Francis, Computing Lab.
Aberdeen Proving Ground, Maryland 21005

1 Commandant
U. S. Army Air Defense School
Attn: Missile Sciences Division, C&S Dept.
P. O. Box 9390
Fort Bliss, Texas 79916

1 Commanding General
U. S. Army Missile Command
Attn: Technical Library
Redstone Arsenal, Alabama 35809

1 Commanding General
Frankford Arsenal
Attn: SMUFA-1310 (Dr. Sidney Ross)
Philadelphia, Pennsylvania 19137

1 Commanding General
Frankford Arsenal
Attn: SMUFA-1300
Philadelphia, Pennsylvania 19137

1 U. S. Army Munitions Command
Attn: Technical Information Branch
Picatinney Arsenal
Dover, New Jersey 07801

1 Commanding Officer
Harry Diamond Laboratories
Attn: Mr. Berthold Altman
Connecticut Avenue and Van Ness St.,N.W.
Washington, D. C. 20438

1 Commanding Officer
Harry Diamond Laboratories
Attn: Library
Connecticut Avenue and Van Ness St.,N.W.
Washington, D. C. 20438

1 Commanding Officer
U. S. Army Security Agency
Arlington Hall
Arlington, Virginia 22212

1 Commanding Officer
U. S. Army Limited War Laboratory
Attn: Technical Director
Aberdeen Proving Ground
Aberdeen, Maryland 21005

1 Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

1 Director
U. S. Army Engineer Geodesy,
Intelligence & Mapping
Research and Development Agency
Fort Belvoir, Virginia 22060

1 Commandant
U. S. Army Command and General Staff College
Attn: Secretary
Fort Leavenworth, Kansas 66207

1 Dr. H. Robl, Deputy Chief Scientist
U. S. Army Research Office (Durham)
Box CM, Duke Station
Durham, North Carolina 27706

1 Commanding Officer
U. S. Army Research Office (Durham)
Attn: CRD-AA-IP (Richard O. Ulsh)
Box CM, Duke Station
Durham, North Carolina 27706

1 Superintendent
U. S. Army Military Academy
West Point, New York 10996

1 The Walter Reed Institute of Research
Walter Reed Army Medical Center
Washington, D. C. 20012

1 Commanding Officer
U. S. Army Electronics R&D Activity
Fort Huachuca, Arizona 85163

1 Commanding Officer
U. S. Army Engineers R&D Laboratory
Attn: STINFO Branch
Fort Belvoir, Virginia 22060

1 Commanding Officer
U. S. Army Electronics R&D Activity
White Sands Missile Range, New Mexico 88002

1 Director
Human Resources Research Office
The George Washington University
300 N. Washington Street
Alexandria, Virginia 22300

1 Commanding Officer
U. S. Army Personnel Research Office
Washington, D. C.

1 Commanding Officer
U. S. Army Medical Research Laboratory
Fort Knox, Kentucky 40120

1 Commanding General
U. S. Army Signal Center and School
Fort Monmouth, New Jersey 07703
Attn: Chief, Office of Academic Operations

1 Dr. S. Benedict Levin, Director
Institute for Exploratory Research
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

1 Director
Institute for Exploratory Research
U. S. Army Electronics Command
Attn: Mr. Robert O. Parker, Executive
Secretary, JSTAC (AMSEL-XL-D)
Fort Monmouth, New Jersey 07703

1 Commanding General
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

Attn: AMSEL-SC
RD-D
RD-G
RD-MAF-I
RD-MAT
RD-GF
RD-MN (Marine Corps LnO)
XL-D
XL-E
XL-C
XL-S
HL-D
HL-L
HL-J
HL-P
HL-O
HL-R
NL-D
NL-A
NL-P
NL-R
NL-S
KL-D
KL-E
KL-S
KL-T
VL-D
WL-D

1 Mr. Charles F. Yost
Special Assistant to the Director
of Research
National Aeronautics & Space Admin.
Washington, D. C. 20546

1 Director
Research Laboratory of Electronics
Massachusetts Institute of Technology
Cambridge, Massachusetts 02139

1 Polytechnic Institute of Brooklyn
55 Johnson Street
Brooklyn, New York 11201
Attn: Mr. Jerome Fox
Research Coordinator

1 Director
Columbia Radiation Laboratory
Columbia University
538 West 120th Street
New York, New York 10027

1 Director
Stanford Electronics Laboratories
Stanford University
Stanford, California 94301

1 Director
Electronics Research Laboratory
University of California
Berkeley, California 94700

1 Director
Electronic Sciences Laboratory
University of Southern California
Los Angeles, California 90007

1 Professor A. A. Dougal, Director
Laboratories for Electronics
and Related Science Research
University of Texas
Austin, Texas 78712

1 Professor J. K. Aggarwal
Department of Electrical Engineering
University of Texas
Austin, Texas 78712

1 Division of Engineering and Applied Physics
210 Pierce Hall
Harvard University
Cambridge, Massachusetts 02138

Security Classification

DOCUMENT CONTROL DATA R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author)

University of Illinois
Coordinated Science Laboratory
Urbana, Illinois 61803

2a. REPORT SECURITY CLASSIFICATION
Unclassified

2b. GROUP

3. REPORT TITLE

A DECODING METHOD FOR BOSE-CHAUDHURI BINARY CODES USING AN ERROR COUNTING TECHNIQUE

4. DESCRIPTIVE NOTES (Type of report and inclusive dates)

5. AUTHOR(S) (Last name, first name, initial)

Bouknight, W. Jack

6. REPORT DATE October, 1965	7a TOTAL NO. OF PAGES 29	7b. NO. OF REFS. 6

8a. CONTRACT OR GRANT NO.
DA 28 043 AMC 00073(E)

b. PROJECT NO.
20014501B31F

c. Also National Science Foundation

d. under Grant NSF GK-36

9a. ORIGINATOR'S REPORT NUMBER(S)
R-267

9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES

Qualified requesters may obtain copies of this report through DDC.
May be released to OTS.

11. SUPPLEMENTARY NOTES

12. SPONSORING MILITARY ACTIVITY
U. S. Army Electronics Command
Fort Monmouth, New Jersey 07703

13. ABSTRACT

The implementation of a decoding scheme for Bose-Chaudhuri (n,K) cyclic codes is discussed. A method of error counting is formulated and a trial-and-error correction operation is developed based on error count reduction by successful trial corrections

DD FORM 1 JAN 64 1473

Security Classification

Security Classification

KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
error-correction Bose-Chaudhuri error-counting						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization (corporate author) issuing the report.

2a. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2b. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7a. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7b. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8a. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8b, 8c, & 8d. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9a. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9b. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers (either by the originator or by the sponsor), also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through

________________________________."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through

________________________________."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through

________________________________."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring (paying for) the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as (TS), (S), (C), or (U).

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, roles, and weights is optional.

Security Classification