NORTHEASTERN UNIVERSITY

COMMUNICATIONS RESEARCH GROUP

QUARTERLY PROGRESS REPORT NO. 1

Period Covered: 1 September 1965 through 30 November 1965

Date Submitted: 10 December 1965

for

Grant NGR-22-011-013

Stephen J. O'Neil
Grant Monitor

Sponsored by Electronics Research Center, NASA

This report is intended for internal management uses of the grantee and the NASA.

Submitted for the staff by

Sze-Hou Chang

Sze-Hou Chang
Principal Investigator

1. Investigations Being Undertaken and Planned

(a) Present Work

The objectives of the research work supported by this grant are two-fold. (1) To conduct a review of information theory literature pertinent to the application in the digital data system used for aerospace guidance. (2) To perform theoretical analysis necessary to demonstrate how the range, capacity, reliability, and efficiency of a digital data transmission system can be improved.

During this period, emphasis is on item (2). Item (1) will be covered in more detail during the next period when a graduate research assistant joins this group. He will be assigned the initial phase of survey work and the liasson work with the Electronic Research Center.

Four items of work, in the area of (i) Data Rate versus Intersymbol Interference; (ii) Design of Orthogonal Codes; and (iii) Error Control Codes; and (iv) A technique for bandwidth compression in telemetry are reported below.

(i)--A Study of Transmission Rate Versus Intersymbol Interference

We assume a digital transmission system as in Figure 1 in which a signal $s_1(t)$ is transmitted over the channel every T seconds with a plus or minus polarity. The channel distorts $s_1(t)$ into a known $s(t)$ and then adds white gaussian noise. We assume that the problem is scaled such that $s(t)$, the distorted signal before noise addition, lasts for exactly one second and such that the noise power is one watt. The information bit stream, represented by the polarity of $s(t)$, is to be detected by matched filter techniques in the data processor.

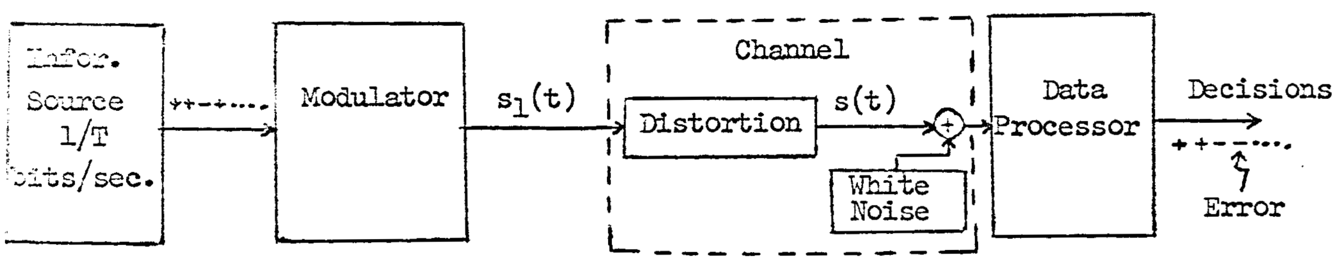


Figure 1 Digital Transmission System

For $T \geq 1$ there is no overlap between successive received signals and the per-symbol probability of error, P_e, depends only on the signal energy.[1] To this P_e there corresponds an overall channel capacity C_1 in bits-per-channel-use.* To maximize the capacity in bits-per-second C under the constraint $T \geq 1$ one should set $T = 1$, that is, transmit as rapidly as possible without causing intersymbol interference.

If one tries to transmit at a faster rate, that is $T < 1$, then he introduces intersymbol interference and the individual bits are no longer easily recognized. See Figure 2. Further, P_e is increased and the channel capacity in bits-per-channel-use is decreased. The increased transmission rate may, however, more than compensate for this preliminary loss in the first computation of C, the capacity in bits-per-second. Thus, we are led to investigate if there exists an optimum choice of T to maximize C for a known s(t).

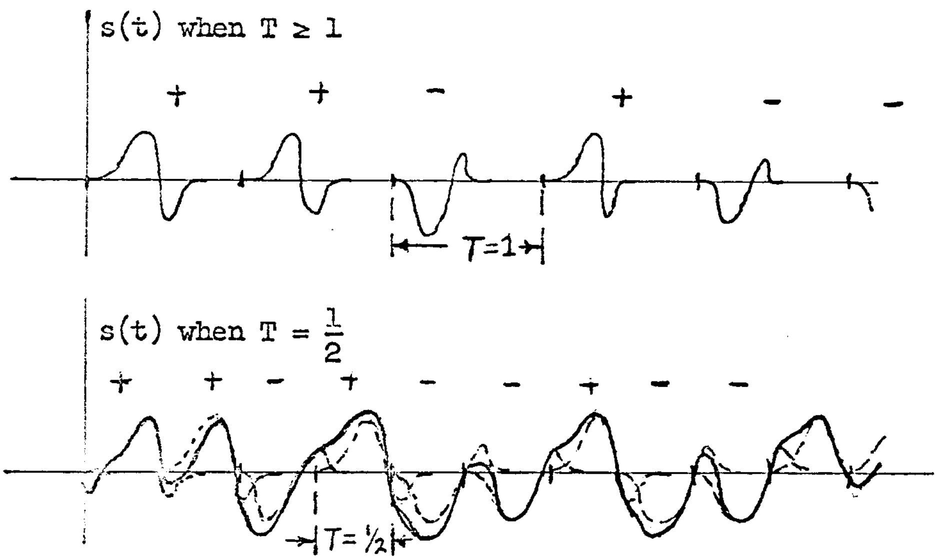


Figure 2 Received Signal Before Noise Addition

Casting the problem in a different light, suppose we are transmitting at a source rate greater than one symbol per second, yielding a poor per-symbol P_e because of intersymbol interference. We contemplate slowing the source rate to cut down the interference, hoping to improving our overall system performance. Clearly this is identical to the problem stated above if the criterion is to maximize the overall system capacity C.

Let us limit the parameter T to the range $\frac{1}{2} \leq T \leq 1$ to represent, at most, a doubling of the transmission rate. (This also limits intersymbol

---

*One uses the well-known formula: $C_1 = 1 + P_e \log P_e + (1-P_e) \log(1-P_e)$

interference to adjacent symbols only.) If we further assume a matched filter detection scheme which subtracts out the channel memory (MacColl's scheme or, equivalently Aein and Hancock's "switched mode" detector[2]), then we can calculate P_e.[3] From this P_e we calculate the channel capacity in bits-per-channel-use (for a binary symmetric channel) and, multiplying by $1/T$, we have C in bits-per-second.

The results of these calculations for a general $s(t)$ with auto-correlation function $\phi(\tau)$ are presented in Figure 3. In that Figure the abscissa ρ is the signal energy on $0 < t < T$:

$$\rho = \int_0^T s^2(t)\, dt;$$

the parameter r represents the correlation of $s(t)$ on $0 < t < T$ with the remainder of $s(t)$:

$$r = \frac{\int_0^T s(t)\, s(t+T)\, dt}{\int_0^T s^2(t)\, dt} = \frac{\phi(T)}{\rho};$$

and the ordinate TC is the capacity in bits-per-channel-use. For a given $s(t)$ lasting from 0 to 1 second, one computes ρ and r as functions of T and then uses Figure 3 to evaluate C for selected values of T. A few (say 5) such evaluations outlines a plot of C vs. T from which one can extract the optimum T(for $1/2 < T < 1$).

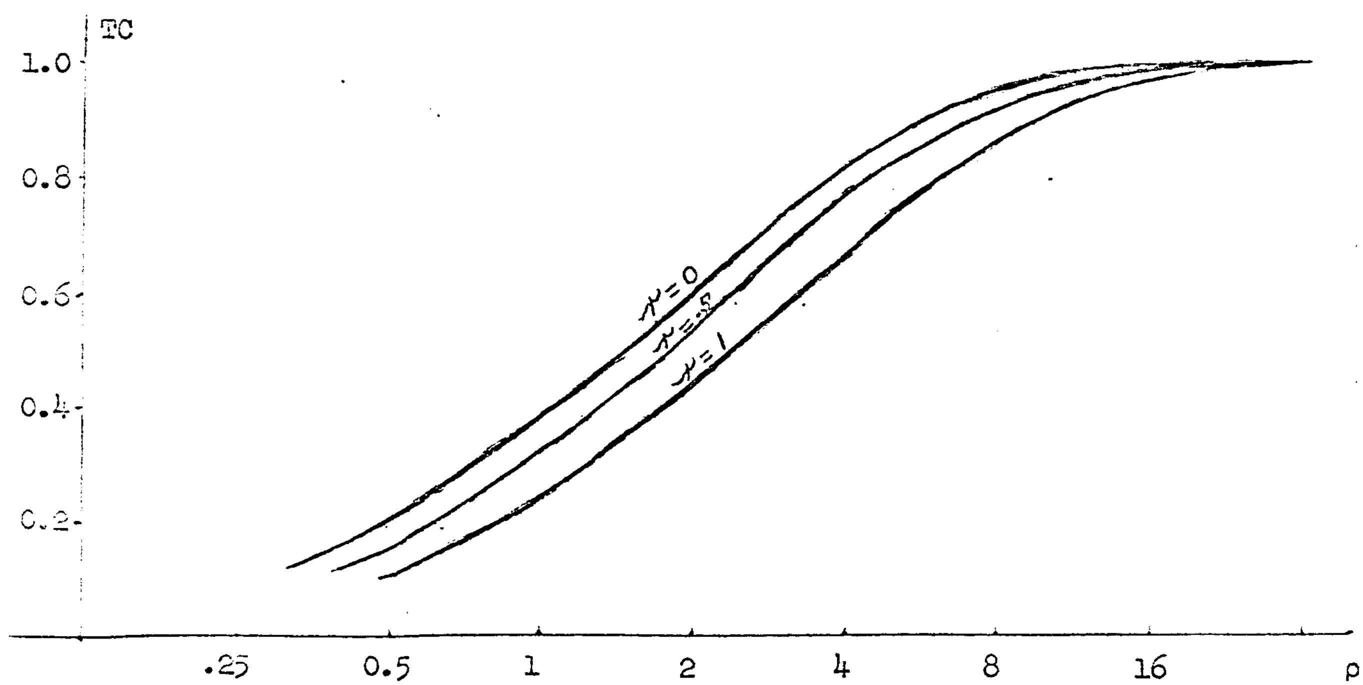


Figure 3 Bits-per-channel-use vs. Usable Signal Energy

As a very simple example of the procedure, we assume the $s(t)$ of Figure 4a.

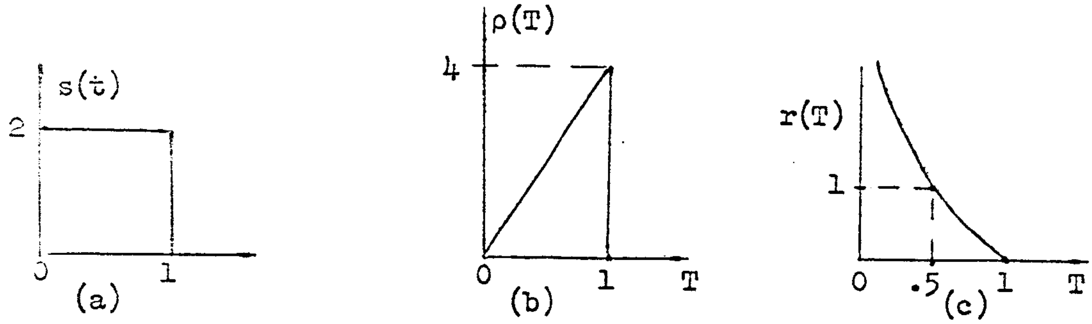


Figure 4 Received Signal $s(t)$ and Parameters ρ and r

In Figure 4b we plot $\rho(T)$ and in Figure 4c we have $r(T) = \frac{1-T}{T}$. With the aid of Figure 1 we are now able to plot C vs. T as shown in Figure 5. We see that the optimum T is approximately T = .70, and that this choice of T represents a 19% bit-per-second increase of the capacity over T = 1 second.

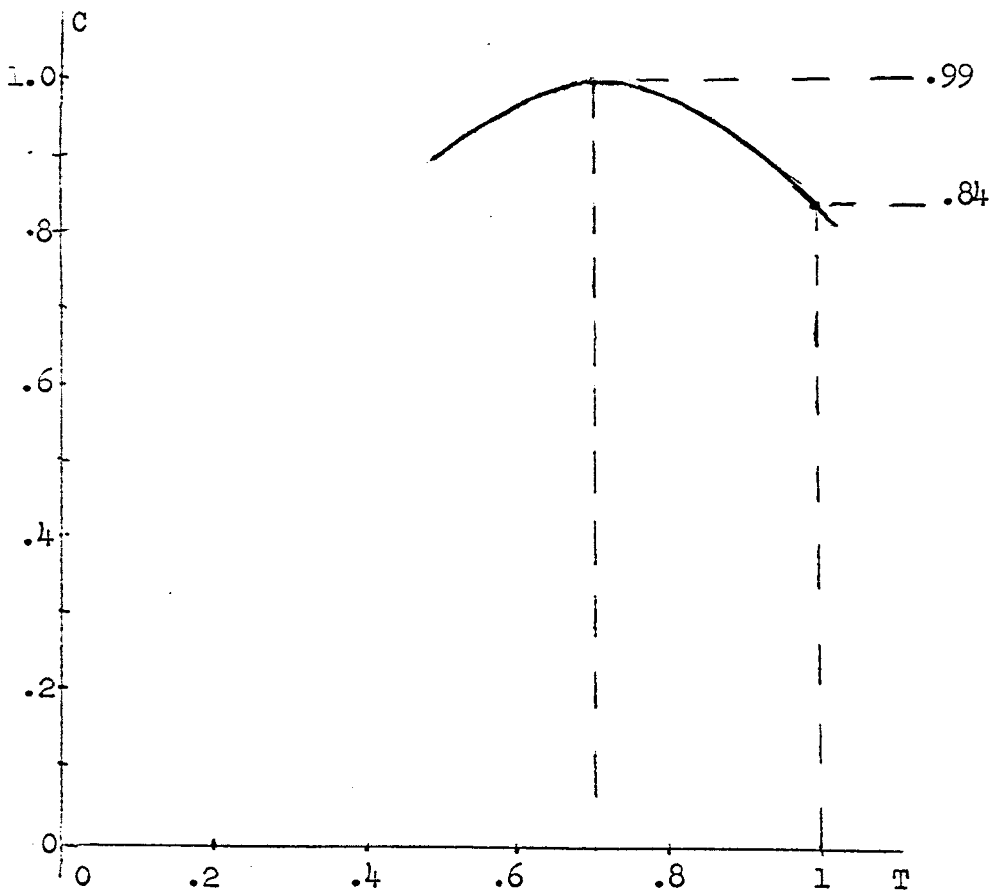


Figure 5 Capacity vs. T

The foregoing illustrates that in some cases it is profitable to increase the transmission rate to the point where some intersymbol interference is created if one has the receiver to cope with this interference. A simple method of evaluating that rate which optimizes channel capacity is presented.

References

1. C. W. Helstrom, Statistical Theory of Signal Detection, Pergamon Press, New York, 1960.

2. J. M. Aein and J. C. Hancock, "Reducing the Effects of Intersymbol Interference with Correlation Receivers", IEE Transactions on Information Theory, (July 1963).

3. R. A. Gonsalves, unpublished notes under Contract AF19(628)-3312, Northeastern University, June 1965.

(ii)--Design of Orthogonal Codes

In digital communication systems, if a sequence of n digits is used to represent a particular code word, then one can construct (n-1) additional code words, all of which are orthogonal in the n-dimensional space. The orthogonality is expressed by the fact that the inner product of each code vector by itself is a constant and the inner product between two different code vectors is zero. If the detection of each code vector is by computing such inner products automatically by means of digital matched filters, then the chance of making a wrong identification is minimized by the use of an orthogonal set of vectors for code words.

The technique of constructing binary orthogonal code words is well known. The matrix describing an orthogonal binary vector set is called the Hadamard matrix, an example of which is as follows:

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 & 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & -1 & 1 \\ 1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\ 1 & -1 & 1 & -1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 \\ 1 & -1 & -1 & 1 & -1 & 1 & 1 & -1 \end{bmatrix}.$$

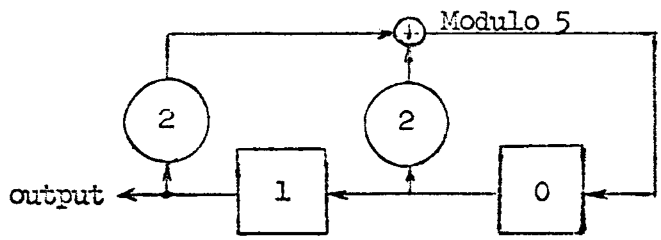
Note that

$$HH^T = \begin{bmatrix} n & & & & & \\ & n & & & O & \\ & & n & & & \\ & & & \cdot & & \\ & O & & & \cdot & \\ & & & & & \cdot \\ & & & & & & n \end{bmatrix} = \lambda I, \quad \text{where} \quad \lambda = n \, .$$

It is desirable that similar orthogonal matrices be constructed for the case where more than two elements +1 and -1 are used. This will lead to orthogonal vectors consisting of digits which are elements of more than two levels. Three methods are explored during this period: (1) construction by means of pseudo-random sequence; (2) construction by inspection; and (3) construction by recursion.

(1) <u>Construction by Means of Pseudo-Random Sequence</u>

A pseudo-random sequence can be generated by a shift register circuit such as follows.



A typical sequence of 24 digits is

1 0 2 -1 2 2 -2 0 1 2 1 1 -1 0 -2 1 -2 -2 2 0 -1 -2 -1 -1.

This sequence has some random properties. First, except for the element 0 (4 in number), the other elements ± 1, ± 2 each has an equal number of occurrences, namely 5. Secondly, the correlations between this sequence and its cyclic shifts are all zero except the sequence with 12 shifts. One may list the original sequence as the first row together with its 11 successive shifts as the succeeding rows. Then retain only the first 12 columns of the array. The result is a 12×12 matrix, as follows:

$$A = \begin{bmatrix}
1 & 0 & 2 & -1 & 2 & 2 & -2 & 0 & 1 & 2 & 1 & 1 \\
-1 & 1 & 0 & 2 & -1 & 2 & 2 & -2 & 0 & 1 & 2 & 1 \\
-1 & -1 & 1 & 0 & 2 & -1 & 2 & 2 & -2 & 0 & 1 & 2 \\
-2 & -1 & -1 & 1 & 0 & 2 & -1 & 2 & 2 & -2 & 0 & 1 \\
-1 & -2 & -1 & -1 & 1 & 0 & 2 & -1 & 2 & 2 & -2 & 0 \\
0 & -1 & -2 & -1 & -1 & 1 & 0 & 2 & -1 & 2 & 2 & -2 \\
2 & 0 & -1 & -2 & -1 & -1 & 1 & 0 & 2 & -1 & 2 & 2 \\
-2 & 2 & 0 & -1 & -2 & -1 & -1 & 1 & 0 & 2 & -1 & 2 \\
-2 & -2 & 2 & 0 & -1 & -2 & -1 & -1 & 1 & 0 & 2 & -1 \\
1 & -2 & -2 & 2 & 0 & -1 & -2 & -1 & -1 & 1 & 0 & 2 \\
-2 & 1 & -2 & -2 & 2 & 0 & -1 & -2 & -1 & -1 & 1 & 0 \\
0 & -2 & 1 & -2 & -2 & 2 & 0 & -1 & -2 & -1 & -1 & 1
\end{bmatrix} .$$

This is an orthogonal matrix, using elements 0, ±1, and ±2. The orthogonality can be verified by finding the product,

$$AA^T = \lambda I$$

where

$$\lambda = 5[1^2 + 2^2] = 25.$$

This type of construction has been found applicable to other primes such as 3, 7 and 11 number of elements. For primes higher than 11, the method requires certain elements in the field of irrational numbers.

(2) Construction by Inspection

The following orthogonal matrices are obtained by inspection

$$\begin{bmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} a & b & -c & d & e & f & g & h \\ -b & a & d & c & -f & e & -h & g \\ c & -d & a & b & -g & h & e & -f \\ -d & -c & -b & a & -h & -g & f & e \\ -e & f & g & h & a & -b & c & -d \\ -f & -e & -h & g & b & a & -d & -c \\ -g & h & -e & -f & -c & d & a & -b \\ -h & -g & f & -e & d & c & b & a \end{bmatrix}$$

By substituting a suitable number for each letter, orthogonal matrices of various number of elements are obtained.

(3) Recursive Method

If A and B are n × n orthogonal matrices, then

(a) $\begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \otimes A$ is a 2n × 2n orthogonal matrix with the same elements as A;

(b) $\begin{bmatrix} a & b \\ -b & a \end{bmatrix} \otimes A$ is a 2n × 2n orthogonal matrix with different elements as A;

(c) $\begin{bmatrix} A & B \\ -B^T & A^T \end{bmatrix}$ is a 2n × 2n orthogonal matrix with the same elements as A and B provided AB = BA.

(iii)--Implementation of an Error-Locating Code

The function of an error-locating code is to locate any subblocks that are in error. It combines two known codes C_1 and C_2 according to certain rules such that one code, C_2, detects the errors in subblocks and the other code, C_1, pinpoints these erroneous subblocks. If C_1 and C_2 are cyclic, the implementation of the code can be done by employing shift registers, modulo two adders, and gates.

Consider a cyclic (7,4) Hamming code. The parity check matrix of the code can be written as

$$H_1 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

This code can either (1) correct a single random error, or (2) detect two random errors in a block size of seven units. For simplicity of illustration, we will use this code for both C_1 and C_2. As C_2, it will detect two random errors in a subblock of 7 digits. As C_1, it will pinpoint an erroneous subblock among 7 subblocks. Thus, for a total number of $7 \times 7 = 49$ binary digits, divided into 7 subblocks, the combined code will locate any single subblock that has two or less digits in error. These 49 digits contain 40 information digits and 9 check digits. The checking equations are contained in the following check matrix which is a tensor product of two component check matrices.

$$H = H_1 \otimes H_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \otimes H_2$$

$$= \begin{bmatrix} H_2 & 0 & 0 & H_2 & 0 & H_2 & H_2 \\ 0 & H_2 & 0 & H_2 & H_2 & H_2 & 0 \\ 0 & 0 & H_2 & 0 & H_2 & H_2 & H_2 \end{bmatrix}$$

When $H_2 = H_1$ is substituted into the expression, it becomes a 9×49 matrix. Both encoding and decoding can be performed by computing the inner products of the message sequence of 49 digits with the 9 rows of the check matrix. These computations yield the values of the 9 check digits in encoding or the values of the 9 syndrome digits in decoding. In case of cyclic codes, such computations can be implemented in the form of shift registers. The circuits for encoder and decoder are almost identical.

Figure 1 shows such a circuit. Depending on the functions and timings of the gates, this circuit can be used either as an encoder or decoder.

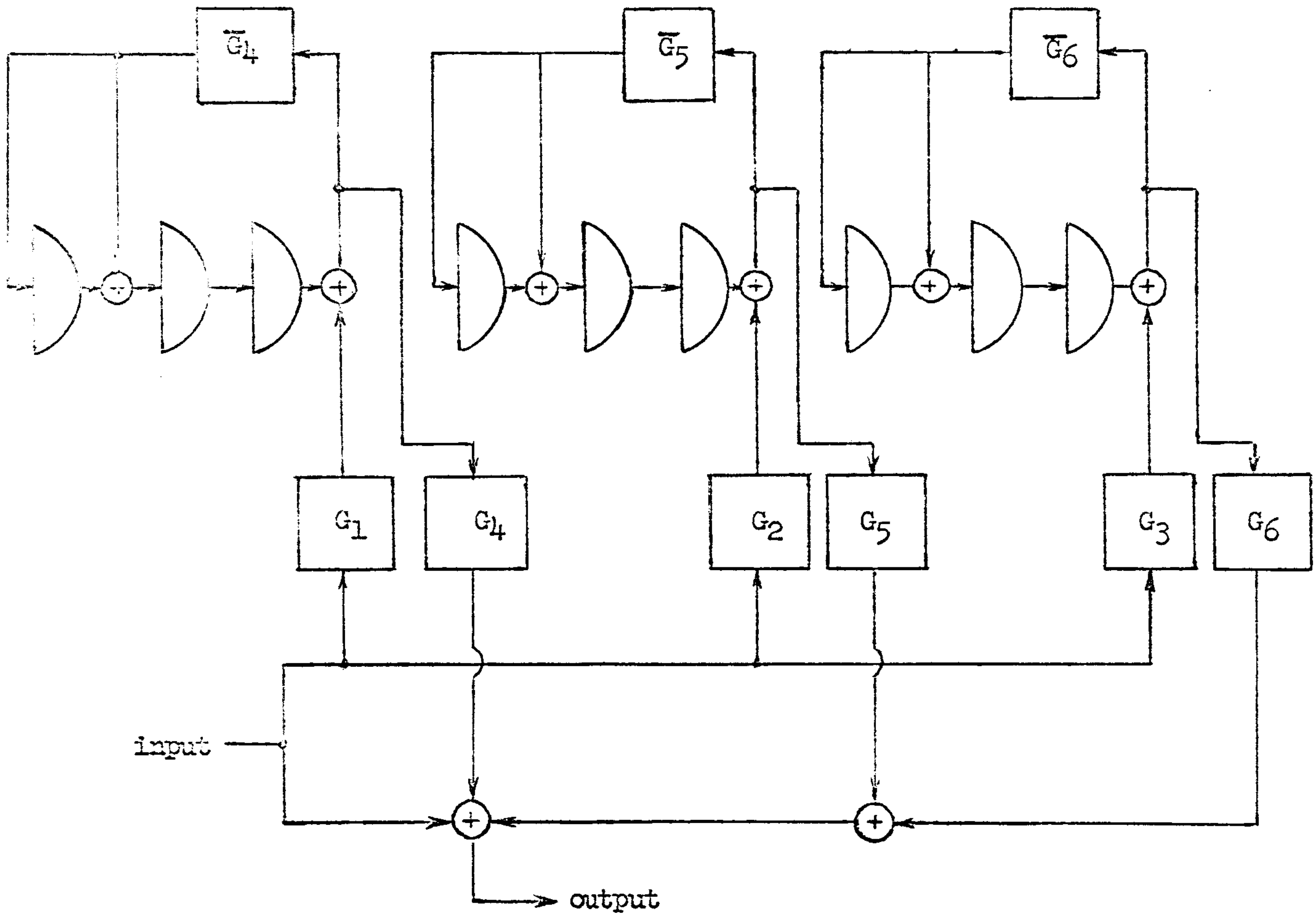


Figure 1 A.Circuit for the Encoder and Decoder of Code

$$H = H_1 \otimes H_2, \quad H_1 = H_2 = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

When used as an encoder the gates are synchronized according to Table 1.

Time \ Gate	G_1	G_2	G_3	G_4	$\overline{G}_4$	G_5	$\overline{G}_5$	G_6	$\overline{G}_6$
$0^+ - 7T^-$	1	0	1	0	1	0	1	0	1
$7T^+ - 14T^-$	1	1	1	0	1	0	1	0	1
$14T^+ - 21T^-$	1	1	0	0	1	0	1	0	1
$21T^+ - 28T^-$	0	1	1	0	1	0	1	0	1
$28T^+ - 32T^-$	1	0	0	0	1	0	1	0	1
$32T^+ - 35T^-$	0	0	0	1	0	0	1	0	1
$35T^+ - 39T^-$	0	1	0	0	1	0	1	0	1
$39T^+ - 42T^-$	0	0	0	0	1	1	0	0	1
$42T^+ - 46T^-$	0	0	1	0	1	0	1	0	1
$46T^+ - 49T^-$	0	0	0	0	1	0	1	1	0

Table 1 Encoder Timing for Gates of Figure 1
(1 denotes gate closed and 0 gate open)

The inputs are fed in during $0 - 32T^-$, $35T^+ - 39T^-$, and $42T^+ - 46T^-$, where T is the time interval for one digit. "+" signifies the beginning of a time interval and "-" the end of that interval. No inputs are fed in during $32T^+ - 35T^-$, $39T^+ - 42T^-$, and $46T^+ - 49T^-$. The total input digits for each block are, therefore, 40 digits. The output sequence contains two parts: information digits and checking digits. The information digits are identical to the input digits. The positions for the checking digits are 33rd, 34th, 35th, 40th, 41st, 42nd, 47th, 48th, and 49th positions. There are altogether 49 digits for each encoded block.

Now, consider Figure 1 as a decoder. The input is fed at the same place, but the outputs are taken from the 9 stages of the shift register. There is no need for gates G_4, G_5, and G_6, hence they are left open. On the other hand, $\overline{G}_4$, $\overline{G}_5$, and $\overline{G}_6$ are always closed. The timing for gates G_1, G_2 and G_3 are listed in Table 2.

Time \ Gates	G_1	G_2	G_3
$0^+ - 7T^-$	1	0	1
$7T^+ - 14T^-$	1	1	1
$14T^+ - 21T^-$	1	1	0
$21T^+ - 28T^-$	0	1	1
$28T^+ - 35T^-$	1	0	0
$35T^+ - 42T^-$	0	1	0
$42T^+ - 49T^-$	0	0	1

Table 2 Decoder Timing for Gates of Figure 1

There are 49 digits in each received block which are fed successively into the input of the decoder. At the end of each block, we investigate the remainder at each stage of the shift register. If all of them are zeros, we assume no error in the block just received. Otherwise, there are some erroneous digits in it. The procedure of locating the subblock in error is as follows:

(1) Divide the block of 49 into 7 subblocks of 7 digits each.

(2) Group the 9 shift register stages into 3 groups. Label the first three from right S_1, the second three from right S_2, and the last three S_3.

(3) Assign a value 0 to S_i, for i = 1, 2, or 3, if 3 shift register stages in that group all have zero remainders. Otherwise, assign a value 1 to S_i.

(4) The following matrix contains all possible combination of S_i which is the same as the parity check matrix of code C_1, i.e., H_1.

<u>Remainder Representation</u>

S_1	0	1	0	0	1	0	1	1
S_2	0	0	1	0	1	1	1	0
S_3	0	0	0	1	0	1	1	1
Subblock #		7	6	5	4	3	2	1 .

For instance, if $(S_1\ S_2\ S_3) = (110)$ the 4^{th} subblock contains one or two corrupted digits, but the exact positions of the errors are not known. It is evident that $(S_1\ S_2\ S_3) = (000)$ denotes no error whatsoever.

So far, we have demonstrated the idea and implementation of error-locating codes. If the parity check matrix elements are allowed to be expressed first in the extension fields of binary field and then translated back to the binary field, more variaties and more efficient codes may result. The idea of combining two known codes may also be applied to the product of two known generator matrices. The advantage of such a product is that the Hamming distance of the new code is equal to the product of that of the two original codes. With increased distance the code is capable of correcting or detecting more errors.

(iv)--A Technique of Bandwidth Compression in Telemetry*

An attempt is being made to define the problems associated with an analytic study of the following type of telemetry bandwidth compression technique.[1] An unknown random process $x(t)$ is periodically sampled at times $t_n \equiv t_o + n\Delta t$, $n = 0,1,\dots$. At $n = 0$, the value of the process, $x(t_o)$, is noted and placed in a buffer for future transmission, as is the value of t_o. An aperture, defined by the boundaries $x(t_o) + \Delta$ and $x(t_o) -\Delta$ is symmetrically placed about $x(t_o)$. As long as $x(t_n)$ falls within the aperture, no action is taken. At the first n, say i, such that $x(t_i)$ falls outside the aperture, the values of $x(t_i)$ and i are placed in a buffer for future transmission and the aperture is moved to $x(t_i)\pm\Delta$. The sampling process is then continued.

It is evident that this technique will generate a set of sample representation points $\{x(t_i)\}$ and times $\{t_i\}$ such that the sampled process can be reproduced to within a tolerance of $\pm\Delta$ at any sample point. Furthermore, the buffering of the $\{x(t_i)\}$ and $\{t_i\}$ will allow the sample representation points to be transmitted at a uniform rate. Thus this technique can be used as a bandwidth compression technique in telemetry.

Results to Date

The specific case of $x(t)$ being a first order Markov process is being studied. The analytic techniques which have been used are as follows.

(1) For the limiting case of $\Delta t \to 0$, $n \to \infty$ such that $t_o + n\Delta t \to t$, given that $x(t)$ is stationary and continuous, one can study the bandwidth compression technique as a boundary value problem associated with the solution of the two Kolmogorov equations.[2] We have found the solution for the mean time between transmitted samples for the specific case of $x(t)$ being a Gauss-Markov process.

---

*This work is being performed by Leonard Ehrman at Northeastern University under an NSF fellowship for Ph.D. candidates.

(2) For the case in which $x(t)$ can assume only a discrete set of values, $\{X_i\}$, the $x(t_n)$ process forms a first-order Markov chain.[3] The mean transmission rate can be determined through a study of the transition matrix of the chain. For the case in which $x(t)$ is continuous in amplitude, one can form a chain which approximates the continuous process by quantizing the aperture space and defining the elements of the transition matrix through integrals of the conditional probability density function of the continous process.

Work to be Performed

In the future, the following problems will be studied:

(1) What can be said of the technique when the input is a higher-order Markov process.

(2) How can zero-crossing analysis techniques be extended to or applied to the solution of this problem for more general input processes.

(3) How does one analyze an interpolative, as opposed to a predictive, compression technique.

References

1. E. Medlin, "Sampled Data Prediction for Telemetry Bandwidth Compression", IEEE Transactions on Space Electronics and Telemetry, vol. SET-11, No. 1, (March 1965), p. 29.

2. D. Middleton, An Introduction to Statistical Communication Theory, McGraw-Hill Co., New York, Sec. 10, 1960.

3. E. Parzen, Stochastic Processes, Holden-Day, Inc., San Francisco, 1962, p. 188.

2. Papers Submitted

The abstracts of two papers have been submitted for possible presentation at the International Symposium on Information Theory which will take place January 31 through February 2 at the UCLA. They are:

(i) "Dual Product Codes", by Sze-Hou Chang and Lih-Jyh Weng.

(ii) "Note on Orthogonal Matrices Using Integers as Elements", by Sze-Hou Chang.

3. Conferences and Meetings

On September 10, 1965, Stephen J. O'Neil and Jean R. Roy, both of ERC, NASA, visited Northeastern University. They discussed with the Communications Research group on the type and scope of work under the grant as well as the report schedules.

On October 14, 1965, R. A. Gonsalves of Northeastern University, visited the NASA offices in Cambridge to meet with Jean Roy and Jason Adleman of ERC, NASA, and Walter Koe of Engineered Electronics Company (EECO) to inspect an EECO Digital Breadboard. On October 21, 1965, R. A. Gonsalves had a similar meeting with Jason Adleman and Ron Eisenhower of Digital Equipment Corporation.

On October 13, 1965, a project meeting was held at Northeastern University. It was attended by Charles F. Hobbs of AFCRL, Stephen J. O'Neil and Jean Roy of ERC, NASA, Communications Research group of Northeastern University and graduate students. Martin Schetzen and Sze-Hou Chang, both of Northeastern University faculty, presented topics on non-linear system characterization and dual product codes.

On November 4 and 5, Sze-Hou Chang of Northeastern University attended NEREM convention at Boston Sheraton.