XV. PROCESSING AND TRANSMISSION OF INFORMATION*

Prof. E. Arthurs
Prof. P. Elias
Prof. R. M. Fano
Prof. J. Granlund
Prof. D. A. Huffman
Prof. R. C. Jeffrey
Prof. H. Rogers, Jr.
Prof. C. E. Shannon
Prof. W. M. Siebert
Prof. J. M. Wozencraft
Prof. W. A. Youngblood
D. C. Coll
J. E. Cunningham
J. B. Dennis
M. A. Epstein
H. A. Ernst
E. F. Ferretti
R. G. Gallager
T. L. Grettenberg
F. C. Hennie III
E. M. Hofstetter
M. Horstein
T. S. Huang
T. Kailath
R. A. Kirsch
G. E. Mongold, Jr.
D. M. R. Park
J. N. Pierce
B. Reiffen
W. L. Wells
H. L. Yudkin

RESEARCH OBJECTIVES

Many of the activities of this group continue as described in the statement of Research Objectives which appeared here in January 1958.

One of these activities is the statistical investigation of information sources. The main objective is to estimate the rate at which the sources generate information and to determine how to encode their output economically in order to decrease the channel capacity required for transmission. The group is currently continuing such an investigation on pictures as information sources by recording the pictures in digital form for analysis and processing on a digital computer.

A second current objective is the investigation of channels for information transmission. This includes study of the fundamental theoretical relationships between transmission rate, error probability, delay, and equipment complexity, and the construction of suitable coding procedures, especially for binary channels. Efforts are being made to extend some of the results on binary channels to continuous channels, particularly with respect to communication over a time-varying multipath medium. Channels with several input and output terminals are also being investigated.

A current activity in the processing of information is the formulation and investigation of models of systems for the storage and retrieval of information. In particular, emphasis is being placed on the problem of machine selection of subsets, called "bibliographies," from a set of stored documents. A bibliography may be heuristically defined as a set of documents pertinent to a particular topic.

In the design of coding and decoding devices, finite-state binary logical circuits play a critical role. A binary circuit can be considered as a transducer that transforms an input stream of binary digits into a related output stream. In the process, information may be lost and the coded form of the stream changed drastically. Thus a finite-state circuit is a rather general information channel. Study in this area is aimed at understanding how the loss of information in a finite-state circuit depends upon the logical structure of the circuit and upon the solvability of the equations that show how the output is related to the input.

From an alternative point of view, any finite-state circuit classifies each of the infinitely many possible input sequences of digits into one of the finite number of states. Studies made of minimal descriptions of finite-state circuits and of approximate models thereof are important, in that they show how to describe efficiently the patterns of digits in a sequence. More closely applicable to the pattern-recognition problem is a study of logical circuits whose description is most conveniently made in more than one dimension. For example, the study of circuits whose logical elements can be arranged in a uniform planar array like that formed by the squares on an indefinitely large chessboard is particularly pertinent to possible schemes for filtering and logical processing of an

* This research was supported in part by Purchase Order DDL-B222 with Lincoln Laboratory, which is supported by the Department of the Army, the Department of the Navy, and the Department of the Air Force under Contract AF19(122)-458 with M.I.T.

ordinary black and white photograph.

The choice of a code for transmitting information over a channel is dependent upon a knowledge of the channel parameters. When the channel is not stationary or is incompletely specified, a possible operating procedure would be to measure the channel before the transmission of the message. We have recently started an investigation of sequential measurement processes for digital channels. This includes study of the fundamental theoretical relationships between accuracy of measurement and duration of the measurement process.

E. Arthurs, P. Elias, R. M. Fano, D. A. Huffman

A. INFORMATION LOSS ASSOCIATED WITH DECISION-MAKING IN ADDITIVE GAUSSIAN CHANNELS

A recent paper (1) defines the a posteriori probability computing channel (APPCC) which has a set of ℓ inputs that are equal energy signals, each of duration T, confined to bandwidth W (approximately), and mutually orthogonal. After being perturbed by additive white Gaussian noise, a received signal is crosscorrelated with replicas of each of the possible transmitted signals, and the a posteriori probability of each input event is computed. These ℓ a posteriori probabilities or the crosscorrelations from which they are determined are the outputs of the channel. Thus the channel has ℓ discrete inputs, and an output which is an ℓ-tuple each component of which may assume continuous values. It is also shown that the APPCC in tandem with a decision operation is equivalent to a discrete channel, for example, with $\ell = 2$ and a maximum likelihood decision, the binary symmetric channel (BSC) results.

We define the parameter

$$a^2 = \frac{2E}{N_o}$$

where E is the signal energy, and N_o is the noise power per cycle. It is easy to see that for small values of a, Shannon's capacity W log [1 + (S/N)] approaches $a^2/2$ natural units in time T. It has been shown (1) that for small a, the capacity per symbol is

$$C_\ell = \frac{(\ell-1)}{2\ell} a^2$$

natural units.

In the special case $\ell = 2$, if the two transmitted waveforms are selected so that each is the negative of the other and their crosscorrelation is -E, a crosscorrelator receiver can similarly compute the a posteriori probabilities of the two possible inputs. Using primes for this case, we obtain $C_2' = a^2/2 = 2C_2$. That is, the effective signal-to-noise (power) ratio for equal and opposite signals is twice the corresponding ratio for orthogonal signals.

The capacity of the binary symmetric channel is $C_{BSC} = \log 2 + p \log p + (1-p) \log (1-p)$,

where p is the probability of error. If the BSC is thought of as being derived from a binary probability computing channel in tandem with a maximum likelihood decision,

$$p = \frac{1}{2}\left[1 - \operatorname{erf}\frac{a}{2}\right]$$

$$p' = \frac{1}{2}\left[1 - \operatorname{erf}\frac{a}{\sqrt{2}}\right]$$

For small values of a, we may obtain C_{BSC} and C'_{BSC} as a function of a by making use of the series expansion for erf x and log (1+x) with only first- and second-order terms preserved. This results in expressions that are applicable for small values of a^2:

$$C_{BSC} = a^2/2\pi \quad \text{and} \quad C'_{BSC} = a^2/\pi$$

In view of our discussion, we can make the following conclusions for small values of a^2. (The decibel values given below refer to the signal-energy increase that is necessary to obtain the same capacity.)

1. The probability computing channel for two equal and opposite signals has ultimate efficiency. The APPCC is $10 \log_{10}(\ell/\ell-1)$ db less efficient than the ultimate efficiency.

2. The maximum likelihood decision that is made at the output of a binary probability computing channel to create the BSC destroys information equivalent to $10 \log_{10}(\pi/2) \approx 2$ db of signal power.

3. The maximum likelihood decision that is made on the output of the APPCC for arbitrary ℓ to create an ℓ-ary symmetric channel destroys information equivalent to no more than $10 \log_{10} \frac{\pi(\ell-1)}{\ell}$ db. This is based on the observation that for fixed a^2 the capacity of the BSC will be less than the capacity of the ℓ-ary symmetric channel for $\ell > 2$.

4. It is conjectured that the decibel figures in conclusions 2 and 3 are upper bounds over the entire range of a^2. This is based upon the heuristic observation that a decision with high probability of being in error (low values of a) destroys more information than a decision with low probability of being in error (high values of a).

B. Reiffen

References

1. B. Reiffen and H. Yudkin, The a posteriori probability computing channel, Group Report 2G-25-7, Lincoln Laboratory, M.I.T., 12 Sept. 1958.

B. CODING FOR A BINARY ERASURE CHANNEL

A thesis, part of which is discussed in Section XV-C, was completed and submitted to the Department of Electrical Engineering, M.I.T., in partial fulfillment of the

requirements for the degree of Doctor of Science, August 1958. Some of the results of this study have already been reported (1, 2).

M. A. Epstein

References

1. M. A. Epstein, Quarterly Progress Report, Research Laboratory of Electronics, M.I.T., Jan. 15, 1958, p. 100.

2. M. A. Epstein, Algebraic decoding for a binary erasure channel, Technical Report 340, Research Laboratory of Electronics, M.I.T., March 14, 1958.

C. PATTERNS OF DIGITS FOR CONVOLUTION CODES

The problem of choosing the best pattern of information and check digits for a convolution code was investigated.

Information theory has shown that the probability of error in a memoryless channel can be made to approach zero arbitrarily closely if the rate of transmission is below the channel capacity and the code length becomes arbitrarily long. The major problem associated with such codes is the large amount of effort that might be needed to use such codes. A special class of codes called convolution codes (1, 2, 3, 4) are very interesting because, for either the binary symmetric channel or for the binary erasure channel, codes of this class can be coded and decoded with comparatively little effort, and the probability of error for such codes approaches zero with increasing length in the usual manner. A convolution code is a code with the following properties: (a) The transmitted message is made up of information and check digits that are interleaved in some pattern. (b) The information digits are freely chosen at the transmitter and represent the information to be transmitted over the channel. (c) The check digits are redundant digits that are determined in a code of length n by a parity check of some of the information digits in the preceding n - 1 digits.

The reason that convolution codes can be decoded easily is that they can be decoded sequentially. Thus only one digit is decoded at a given time, each digit being decoded in the order of its transmission. Also, each digit is decoded in a series of steps. The n^{th} step of the decoding procedure for a given digit tries to decode by means of the digits up to and including the n^{th} check digit following the digit that is being decoded. The sequence of steps ends whenever the digit is determined within the required probability. The average effort required by a given step increases as the step number increases. However, the probability of reaching a given step decreases rapidly with the step number. Since the average computational requirements are the sum over n of the product of the average effort in step n and the average probability of needing step n, the average computational requirements are much less than the peak computational requirements.

$$\text{Average computational requirements} = \sum_{n} \begin{pmatrix}\text{average require-}\\ \text{ments for step n}\end{pmatrix}\begin{pmatrix}\text{probability of reaching}\\ \text{step n}\end{pmatrix} \tag{1}$$

The rate of a convolution code is defined to be the limit with increasing n of the fraction of the first n digits that are information digits. There are many patterns with the same rate. That is, if we use I to denote an information digit and C to denote a check digit, the pattern IC IC IC ... with alternating information and check digits, the pattern IICC IICC ... with alternating pairs of information and check digits, and the pattern IICC IC IICC IC ..., all have the rate 1/2. Similarly, the patterns IIICC IIICC ..., IICIC IICIC ..., ICIICICIIC, all have the rate 3/5. Different patterns with the same rate have different properties. Thus two questions arise: How can patterns be compared? Which pattern, if any, is preferred over the other patterns?

It has not been possible, in general, to evaluate the probability of error or the computational requirements of specific codes. However, it has been possible to find bounds on the average probability of error and on the average computational requirements of a code selected at random from the set of convolution codes with a given pattern. The bound on the probability of error is independent of the pattern if the rate is fixed. On the other hand, the bound on the average computational requirements is dependent on the pattern even when the rate is fixed. The bound on the average computational requirements for step n of the sequential decoding procedure for digit m is determined by the effective rate of transmission at this point. The effective rate of transmission for digit m is defined as the fraction of the digits between digit m and the n^{th} check digit after digit m that are information digits. (See Fig. XV-1.)

As might be expected, the bound on the average computational requirements

step \ digit	1	2	4
1	$\frac{2}{3}$	$\frac{1}{2}$	$\frac{1}{2}$
2	$\frac{3}{5}$	$\frac{1}{2}$	$\frac{3}{5}$
3	$\frac{5}{8}$	$\frac{4}{7}$	$\frac{4}{7}$
4	$\frac{3}{5}$	$\frac{5}{9}$	$\frac{3}{5}$

Fig. XV-1. Effective rate as a function of the digit number and the step number for the pattern IICICIICICIICIC... .

decreases with decreasing effective rate. Thus, if there are two digits i and j which are such that for each step n the effective rate for digit i is always equal to or smaller

than the effective rate for digit j, the bound on the computational requirements for digit i is smaller than or equal to the corresponding bound for digit j. It follows that the computational requirements for the first digit in the pattern IICIC IICIC ... are as large or larger than the requirements for any other digit in the pattern.

The ability to compare the bounds on the computational requirements of single digits can be used to compare patterns. One reasonable aim is to make the largest of the computational bounds for the digits in a pattern as small as possible. According to this criterion, the preferred pattern is one in which the largest computational bound is as small as or smaller than the largest computational bound for any other pattern with the same rate. It has been shown (4) that in terms of this criterion, when the channel is a binary erasure channel, the following pattern is the preferred pattern of all the patterns with a rate of transmission R. We define n_m as the number of information digits before the m^{th} check digit in the pattern. Then, the preferred pattern satisfies Eq. 2 for all m.

$$\frac{mR}{1-R} \leq n_m < \frac{mR}{1-R} + 1 \tag{2}$$

Thus, the preferred pattern for rate 1/2 is ICIC ICIC ..., and the preferred pattern for rate 3/5 is IICIC IICIC ... .

A simple interpretation can be made of the patterns that satisfy Eq. 2. These patterns make the effective rate approach the rate of the code as closely as possible from above at every step. Moreover, such patterns interleave the information digits and the check digits as uniformly as possible under the constraint that the n_m are integers.

The following argument can be made for the plausibility of using the patterns described by Eq. 2. Block codes, in which the information digits are grouped together and the check digits are grouped together, require much computation. On the other hand, convolution codes, in which the information digits and the check digits are interleaved, require much less computation. Hence, it seems reasonable that a convolution code that has the information digits and the check digits interleaved as uniformly as possible will require the least computation.

M. A. Epstein

References

1. P. Elias, Coding for noisy channels, IRE Convention Record, Part 4, 1955.
2. P. Elias, Coding for two noisy channels, Information Theory, Third London Symposium, Sept. 12-16, 1955, edited by C. Cherry (Academic Press, Inc., New York; Butterworths Scientific Publications, London, 1956).
3. J. M. Wozencraft, Sequential decoding for reliable communication, Technical Report 325, Research Laboratory of Electronics, M.I.T., Aug. 9, 1957.
4. M. A. Epstein, Coding for the binary erasure channel, Sc.D. Thesis, Department of Electrical Engineering, M.I.T., 1958.

D. A BOUND ON THE CROSSCORRELATION FUNCTIONS OF A SET OF BINARY SEQUENCES OF FINITE LENGTH

1. Statement of the Problem

Finite-length, binary sequences of positive and negative pulses form a class of signals that might be used as modulating functions in a communication system employing correlation detection.

Consider a set S of M binary sequences $s_1, s_2, \ldots, s_M$ each of which is N digits long. Let the values of the binary states be +1 and -1. Two members s_i and s_j are said to be a distance d_{ij} apart if they differ in d_{ij} digits.

The unnormalized crosscorrelation, $\phi_{ij}(\tau)$, between two members s_i and s_j for a shift of an integral number of digits, τ, is

$$\phi_{ij}(\tau) = (N-\tau) - 2d_{ij}(\tau) = n(\tau) - 2d_{ij}(\tau) \tag{1}$$

where $n(\tau)$ represents the number of overlapping digits at the particular value of τ that is considered. To simplify the notation, $n(\tau)$ and $d_{ij}(\tau)$ will be written as n and d_{ij}, respectively, but it must be understood that the functional notation is implied.

In a system in which the exact time of arrival of a message is unknown a priori, it is necessary to calculate the correlation between the received signal and each possible transmitted signal for all possible values of τ. It is assumed that detection is performed after the bandpass signal is heterodyned to lowpass, and that maximum-likelihood correlation detection is employed. Since the phase of the correlation envelope is lost in such a detection scheme, the decision element operates on the absolute value of the envelope of the correlation function. The possible transmitted signal that has the correlation envelope peak of largest absolute value is chosen as the actual transmitted signal. To minimize the probability of error in detection, we would like to select an encoding alphabet with the lowest possible peak absolute correlation between members that is consistent with the constraints on sequence length and alphabet size.

As a guide in constructing an alphabet of such sequences, we should know how small the crosscorrelation between members can possibly be made. In this report, two bounds are derived which express a limit below which it is impossible to suppress all crosscorrelation functions. A comparison is made of the relative tightness of the two bounds.

2. Outline of Procedures for Deriving the Bounds. Summary of Results

Let us consider listing in matrix form the correlation coefficients for all possible pairs of the M members and for all integral values of the shift parameter τ. (We need consider only integral values of τ because the correlation functions are linear between these points.) There are $\binom{M}{2} = \frac{M(M-1)}{2}$ unordered pairs of members, and for each pair there are 2N - 1 values of the shift parameter that can possibly yield a nonzero

correlation coefficient. The resulting list is an array of dimensions $\frac{M(M-1)}{2}$ by 2N - 1. If the autocorrelation values at zero shift are excluded, there is one number (or perhaps there are several numbers) in the array with a maximum value, say σ_1.

If such a list is made for a second alphabet of the same length and number of members, this second list will contain a maximum value, say σ_2, that may be different from σ_1.

If lists of this kind are made for all possible M-member alphabets of N digit sequences, each list will have a maximum value, σ. From all of these σ's, there is one (or there may be several) equal to a smallest value. It is this smallest value of σ that we wish to bound.

The first bound, which we shall call the "log M bound," is based upon the idea that as the shifting process is carried out in the calculation of the correlation coefficients, the product sequences are shortened until there are not enough points in the remaining space to allow each member of the alphabet to occupy a different point. In this case, at least two members are completely correlated, and therefore there is at least one correlation coefficient in the set having an absolute value at least as large as log M. (Throughout this report the logarithm is to the base 2.) Expressed symbolically,

$$\left|\phi_{ij}(\tau)\right|_{\text{peak}} \geq \log M + \epsilon = \text{integer} \qquad 0 \leq \epsilon < 1 \tag{2}$$

The second bound is expressed in its most general form as

$$\left\langle \phi_{ij}(\tau) \right\rangle_{\max} \Big|_{\min} \geq n - 4(k_1 + 1) \tag{3}$$

where k_1 is the largest integer that satisfies the expression

$$\sum_{j=0}^{k} \binom{n}{j} \leq \frac{2^{n-1}}{M} \qquad n = N - \tau \tag{4}$$

We shall refer to this bound as the "sphere-packing bound." This designation is prompted by the fact that if 2M hyperspheres of equal radius are packed into the space of 2^n points, the radius of these spheres cannot exceed k_1.

The sphere-packing bound, as expressed by Eqs. 3 and 4, is complete and general. However, this form offers little insight into the behavior of the bound, and the solution of a given problem with the use of these equations requires a long calculation. By exploiting the constraint relationships between parameters, the exact behavior of the bound can be clarified, and for alphabets of practical size, a much simpler expression of the bound can be obtained. The first step toward clarifying the bound behavior is to show that k_1 can never decrease (increase) when n increases (decreases). The next

step is to show that k_1 can never change more than one unit at a time as n changes in unit steps. Finally, we determine the range of k_1 in which this bound has a maximum value. Because of the Diophantine nature of the equations involved, a straightforward algebraic approach cannot be used in locating this maximum. Instead, we bracket the range in which the maximum can occur. We shall show, first, that the maximum can not occur for $k_1 > n/10$, regardless of the alphabet dimensions; and, second, that the maximum can occur for values of k_1 that are at least as large as $n/18$ for very large alphabets.

For alphabets of less than 175,000 members the sphere-packing bound reduces to

$$\phi_{ij}(\tau)\Big\rangle_{\max}\Big|_{\min} \geq n - 4 \tag{5}$$

where n is the largest integer that satisfies the inequality

$$1 + n > \frac{2^{n-1}}{M} \qquad n \leq N \tag{6}$$

This fact is verified by showing that the bound can have a greater value for $k_1 > 0$ than for $k_1 = 0$ only if M exceeds 175,000.

Finally, we shall show that for large alphabets the sphere-packing bound is tighter than the log M bound.

3. Derivation of the log M Bound

The first bound is obtained by making use of the fact that for values of τ that approach the sequence length the number of points in the reduced space is less than the number of members in the alphabet. In this case, two members must occupy the same point, and, therefore, are completely correlated.

Let n be an integer, and let us consider two cases.

Case I: $M = 2^n$ $\qquad n = \log M$

At $N - \tau = n$, there are just enough points to go around; either two or more members are alike or each member has a complement. In either event, there is at least one crosscorrelation coefficient with absolute value equal to n. Expressed mathematically,

$$\left|\phi_{ij}(N-n)\right|_{\text{peak}} \geq n = \log M$$

Case II: $2^n < M < 2^{n+1}$

or

$\log M - 1 < n < \log M$

At $N - \tau = n + 1$, either two or more members are alike or at least one has a complement. Therefore,

$$\left|\phi_{ij}(N - n - 1)\right|_{peak} \geq [1 + \log M]_i$$

By combining the results of Cases I and II, we obtain Eq. 2, which holds for all integral values of M.

4. Derivation of the Sphere-Packing Bound

In the calculation of the second bound, use is made of some results from coding theory; specifically, of ideas similar to those used by Hamming (1) in his work on error-correcting codes.

To correct all patterns of k errors in a binary code, the condition $d \geq 2k + 1$ must be satisfied, where d is the minimum distance between any two code members. Let k_a be the largest number of errors for which all patterns can be corrected in a particular code of M members of length N. Then $d \geq 2k_a + 1$. Since k_a is the largest number of errors for which all patterns can be corrected, it follows that

$$d < 2(k_a + 1) + 1$$

or

$$d \leq 2(k_a + 1) \tag{7}$$

Substituting this value of minimum distance for d_{ij} in Eq. 1, we obtain a lower bound on the maximum crosscorrelation coefficient of the particular alphabet that is considered. This bound is

$$\phi_{ij}(\tau)\Big\rangle_{max} = n - 2d \geq n - 4(k_a + 1) \tag{8}$$

Hamming (1) has shown that for binary codes the number of errors for which all patterns can be corrected is related to the number of members in the set and the length of each member as follows:

$$\sum_{j=0}^{k} \binom{n}{j} \leq \frac{2^n}{M}$$

The problem of correlation-envelope detection differs from error correction in the relationship between a member and its complement. Phase is lost in correlation-envelope detection, with the result that a member and its complement are indistinguishable. Similarly, members that are a small distance from the complement of s_j are as likely to be confused with s_j as members that are the same distance from s_j itself. For each point chosen as a code member from the set of all 2^n points, this chosen point, its complement,

and all other points within hyperspheres of radius k about both the chosen point and its complement must be excluded in the selection of additional messages. Each of the two hyperspheres of radius k consists of $\sum_{j=0}^{k} \binom{n}{j}$ points. Therefore, the requirement to be fulfilled is expressed by Eq. 4.

Let k_1 be the largest integral value of k that satisfies this inequality. Consider the M-member code of length N that allows k_a its maximum value. This maximum value of k_a can be no greater than k_1. Therefore,

$$\phi_{ij}(\tau)\Big\rangle_{max}\Big|_{min} \geq n - 4(k_1 + 1)$$

where n and k_1 are both functions of N, τ, and M as expressed by Eq. 4.

For a particular code, this bound produces a set of values — one for each value of τ. Since we are interested in obtaining as tight a bound as possible, it is the peak value of the correlation function that is significant. We would like to know, then, for what value of k_1 (or n) the expression $n - 4(k_1 + 1)$ is a maximum, realizing that k_1 is a function of n. The functional relationship between k_1 and n, as expressed by Eq. 4, makes a direct approach to an explicit expression for the maximum of $n - 4(k_1 + 1)$ appear unattractive. However, the relationship between k_1 and n can be established in three steps: (a) show that $k_1(\tau) \geq k_1(\tau+1)$; (b) show that $k_1(\tau) \leq k_1(\tau+1) + 1$ (that is, k_1 changes in unit steps); (c) find the range of n for which $k_1(\tau-4) > k_1(\tau)$, where $k_1(\tau)$ is the value of k_1 for the displacement τ.

Through these steps, it will be shown that $n - 4(k_1 + 1)$ can have its maximum value at $k_1 > n/18$ for n sufficiently large, but never at $k_1 > n/10$.

a. Proof that $k_1(\tau) \geq k_1(\tau+1)$

We shall now show that for sequences of fixed length, k_1 cannot increase when the displacement τ between sequences increases. Or, expressed another way, as the number of overlapping digits decreases, k_1 can only decrease or remain constant.

Starting with Eq. 4, which is rewritten here in expanded form for convenience,

$$\sum_{j=0}^{k_1(\tau)} \binom{n}{j} = \left[\binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{k_1(\tau)}\right] \leq \frac{2^{n-1}}{M} \tag{9}$$

we can write the analogous expression

$$\sum_{j=0}^{k_1(\tau+\delta)} \binom{n-\delta}{j} \leq \frac{2^{n-\delta-1}}{M} \qquad \delta = \text{integer} \geq 0 \tag{10}$$

In expanded form, we have

$$2^{\delta}\left[\binom{n-\delta}{0}+\binom{n-\delta}{1}+\cdots+\binom{n-\delta}{k_1(\tau+\delta)}\right]\leq\frac{2^{n-1}}{M} \tag{11}$$

Comparing j^{th} terms of Eqs. 9 and 11, we have the ratio

$$R=\frac{\binom{n}{j}}{2^{\delta}\binom{n-\delta}{j}}=\frac{\frac{n!}{(n-j)!\,j!}}{2^{\delta}\frac{(n-\delta)!}{(n-\delta-j)!\,j!}}$$

$$R=\frac{n}{2(n-j)}\cdot\frac{n-1}{2(n-1-j)}\cdot\frac{n-2}{2(n-2-j)}\cdot\cdots\cdot\frac{n-\delta+1}{2(n-\delta+1-j)}$$

From Eq. 10 and from the fact that $2^{P-1}=\frac{1}{2}\sum_{i=0}^{P}\binom{P}{i}$, it is evident that $j<(n-\delta)/2$. Then the last factor in R is less than one; that is

$$\frac{n-\delta+1}{2(n-\delta+1-j)}\leq\frac{n-\delta+1}{n-\delta+2}<1$$

Adding one to the numerator and two to the denominator of a ratio less than one reduces its value; hence, the last term in R is the largest term. Since this largest term is less than one, $R<1$. Therefore, $k_1(\tau)\geq k_1(\tau+1)$.

b. Proof that k_1 Changes in Unit Steps

We now wish to show that k_1 can never change more than one unit at a time as τ (and correspondingly, $n=N-\tau$) changes in unit steps. Examination of Eq. 3 shows that for $k_1\geq n/4$ the correlation bound is negative and has no useful significance. Our interest, then, is confined to the range for which $k_1<n/4$. Again, making use of Eq. 4, we have

$$\sum_{j=0}^{k}\binom{n}{j}=1+n+\frac{n(n-1)}{2!}+\cdots+\frac{n!}{(n-k)!\,k!}\leq\frac{2^{n-1}}{M} \tag{12}$$

The ratio of the j^{th} term to the $(j-1)^{th}$ term in Eq. 12 is

$$\frac{\binom{n}{j}}{\binom{n}{j-1}}=\frac{\frac{n!}{(n-j)!\,j!}}{\frac{n!}{(n-j+1)!\,(j-1)!}}=\frac{n+1-j}{j}=\frac{n}{j}-1+\frac{1}{j}$$

For $j\leq\frac{n}{4}$,

$$\frac{\binom{n}{j}}{\binom{n}{j-1}} > 3$$

or

$$\frac{\binom{n}{j-1}}{\binom{n}{j}} < \frac{1}{3}$$

Bounding the binomial series by a geometric series yields

$$\sum_{j=0}^{k} \binom{n}{j} \leq \binom{n}{k}\left[1 + \frac{1}{3} + \frac{1}{3^2} + \ldots + \frac{1}{3^k}\right] < \binom{n}{k} \frac{1}{1 - \frac{1}{3}} = \frac{3}{2}\binom{n}{k}$$

or

$$\binom{n}{k} > \frac{2}{3} \sum_{j=0}^{k} \binom{n}{j} \qquad k \leq \frac{n}{4} \tag{13}$$

For $k + 1 \leq \frac{n}{4}$,

$$\sum_{j=0}^{k+1} \binom{n}{j} = \sum_{j=0}^{k} \binom{n}{j} + \binom{n}{k+1} > 4\binom{n}{k} > \frac{8}{3} \sum_{j=0}^{k} \binom{n}{j} \tag{14}$$

Now, again, we let k_1 be the largest integral value of k that satisfies inequality 4. Then, adding a term in the series gives

$$\sum_{j=0}^{k_1+1} \binom{n}{j} = \frac{2^{n-1}}{M} + \epsilon = K \text{ (an integer)} \qquad \epsilon > 0$$

Now, increasing the length by one unit, that is to (n+1), we obtain

$$\sum_{j=0}^{k_1+1} \binom{n+1}{j} > K$$

Adding another term to the series and making use of Eq. 14 yields

$$\sum_{j=0}^{k_1+2} \binom{n+1}{j} > \frac{8}{3}K \qquad K < \frac{2^{n-1}}{M}$$

We observe that by increasing the length (i.e., the parameter n) one unit, the right-hand side of Eq. 4 is doubled; however, an addition of two terms on the left-hand side (i.e., to $k_1 + 2$) increases the left-hand side more than 2 2/3 times. Therefore, for $k_1 < n/4$, k_1 can never change by more than one when n changes by one.

c. Range for Which $k_1(\tau-4) > k_1(\tau)$

Examining the function $n - 4(k_1 + 1)$ with the results of the two previous proofs in mind, we see that when n increases without k_1 changing, the function increases one unit; however, when k_1 also changes, the function decreases three units. The function $n - 4(k_1 + 1)$ then has a behavior pattern similar to that shown in Fig. XV-2.

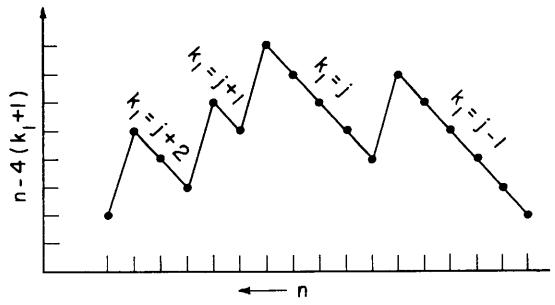

Fig. XV-2. Typical behavior of the bound for $k_1 < n/4$.

In order to establish the range of k_1 in which the bounding function, $n - 4(k_1 + 1)$, has its maximum value, we shall show, first, that this maximum can never occur for $n/10 < k_1(\tau) < n/4$, regardless of the alphabet dimensions. Since the bound is negative for $k_1(\tau) > n/4$, this restricts the maximum of $n - 4(k_1 + 1)$ to the range $k_1(\tau) < n/10$. Later, we shall show that, for sufficiently large alphabet dimensions, the maximum can occur for $k_1(\tau)$ at least as large as $k_1(\tau) = n/18$.

(i) Proof that $k_1(\tau-4) > k_1(\tau)$ for $n(\tau)/10 < k_1(\tau) < n(\tau)/4$

Again, let k_1 be the value of the largest integer k that satisfies inequality 4. It is obvious (see Fig. XV-2) that for the function $n - 4(k_1 + 1)$ to have a larger value for some particular value of k_1, say $k_1 = j$, than for the next smaller value of k_1, $k_1 = j - 1$, k_1 must remain constant at $k_1 = j$ while n increases four or more units. To determine whether or not k_1 does change value when n increases four units, we must determine whether or not the following inequality can be satisfied. (If it can be satisfied, we desire to know for what range of k_1.)

$$\sum_{j=0}^{k_1+1} \binom{n+4}{j} \leq \frac{2^{[(n+4)-1]}}{M} = 16\,\frac{2^{n-1}}{M} \tag{15}$$

We break the sum into two parts:

$$\sum_{j=0}^{k_1+1} \binom{n+4}{j} = \sum_{j=0}^{k_1} \binom{n+4}{j} + \binom{n+4}{k_1+1}$$

Now we introduce a new parameter ϵ with the property that $0 \leq \epsilon < \frac{1}{4}$. Then, by taking the ratio of j^{th} terms, it can be shown that

$$\sum_{j=0}^{k_1} \binom{n+4}{j} < \frac{1}{(1-\epsilon)^4} \sum_{j=0}^{k_1} \binom{n}{j} \leq \frac{1}{(1-\epsilon)^4} \cdot \frac{2^{n-1}}{M} \quad \text{for} \quad k_1 \leq \epsilon n$$

Likewise, it can be shown that

$$\binom{n+4}{k_1+1} < \frac{1}{\epsilon(1-\epsilon)^3} \binom{n}{k_1} < \frac{1}{\epsilon(1-\epsilon)^3} \cdot \frac{2^{n-1}}{M} \quad \text{for} \quad k_1 \geq \epsilon n$$

Then

$$\sum_{j=0}^{k_1+1} \binom{n+4}{j} < \left[\frac{1}{(1-\epsilon)^4} + \frac{1}{\epsilon(1-\epsilon)^3}\right] \frac{2^{n-1}}{M} \quad \text{for} \quad k_1 = \epsilon n \tag{16}$$

The term in brackets

$$\frac{1}{(1-\epsilon)^4} + \frac{1}{\epsilon(1-\epsilon)^3} = \frac{1}{\epsilon(1-\epsilon)^4}$$

is minimum at $\epsilon = 1/5$, has a value of 16 at $\epsilon \approx 0.0925 \approx 1/10.8 < 1/10$, and increases monotonically in between. Then, for k_1 in the range $n/10 < k_1 < n/4$, we have

$$\sum_{j=0}^{k_1+1} \binom{n+4}{j} < \frac{1}{\epsilon(1-\epsilon)^4} \cdot \frac{2^{n-1}}{M} < 16\,\frac{2^{n-1}}{M}$$

We conclude that Eq. 15 is satisfied for k_1 in the range $n/10 < k_1 < n/4$. It follows that the bounding function $n - 4(k_1 + 1)$ has its maximum value for $k_1 < n/10$.

(ii) Proof that the maximum value of $n - 4(k_1 + 1)$ can occur at values of $k_1 > n/18$ for n sufficiently large

At this point, we might suspect that the envelope of the peaks of the bounding function, $n - 4(k_1 + 1)$, is monotonic and that it has its greatest value at $k_1 = 0$. We shall now show that this is not the case, but that the maximum can occur for values of k_1 at least as large as n/18, for large alphabet dimensions. Again we start with Eq. 4

$$\frac{2^{n-1}}{M} \geq \sum_{j=0}^{k} \binom{n}{j} = 1 + n + \ldots + \binom{n}{k}$$

and let k_1 be the value of the largest integer k that satisfies this inequality. This inequality can be converted into an equality by adding a positive quantity Δ. That is,

$$\frac{2^{n-1}}{M} = 1 + n + \ldots + \binom{n}{k_1} + \Delta \qquad \Delta \geq 0 \qquad (17)$$

By modifying parameter values, it will be shown that for $k_1 < n/18$, it is not possible to increase k_1 when n is increased only four units without invalidating the inequality expressed by Eq. 4. These parameter changes will be carried out in two steps. To facilitate identification, let the left-hand side of Eq. 17 and the resulting modifications be identified as LHS. Likewise, identify the right-hand side of Eq. 17 with any resulting modifications as RHS.

First, increase the sequence length by four units, i.e., to n + 4; then the two sides of Eq. 17 become

$$\text{LHS} = 16\,\frac{2^{n-1}}{M}$$

$$\text{RHS} = 1 + (n+4) + \ldots + \binom{n+4}{k_1} + \Delta \geq 1 + n + \ldots + \binom{n}{k_1} + \Delta$$

Now, add a term to the series, and the expressions become

$$\text{LHS} = 16\,\frac{2^{n-1}}{M} \qquad \text{(unchanged)}$$

$$\text{RHS} \geq 1 + n + \ldots + \binom{n}{k_1} + \Delta + \binom{n}{k_1+1}$$

Let $p = (k_1 + 1)/n$. Then

$$\binom{n}{k_1+1} > \left(\frac{1}{p} - 1\right)\binom{n}{k_1}$$

and

$$\text{RHS} > \frac{1}{p}\binom{n}{k_1}$$

By letting $\epsilon = k_1/n$ and bounding the binomial series by a geometric series, we obtain

$$\sum_{j=0}^{k_1}\binom{n}{j} = 1 + n + \ldots + \binom{n}{k_1} < \binom{n}{k_1}\left[1 + \frac{\epsilon}{1-\epsilon} + \left(\frac{\epsilon}{1-\epsilon}\right)^2 + \ldots\right]$$

$$\sum_{j=0}^{k_1}\binom{n}{j} < \binom{n}{k_1}\frac{1}{1-\frac{\epsilon}{1-\epsilon}} = \frac{1-\epsilon}{1-2\epsilon}\binom{n}{k_1}$$

$$\binom{n}{k_1} > \frac{1-2\epsilon}{1-\epsilon}\sum_{j=0}^{k_1}\binom{n}{j}$$

By using this bound on the binomial coefficient, RHS can be bounded as

$$\text{RHS} > \frac{1}{p}\,\frac{1-2\epsilon}{1-\epsilon}\left[1 + n + \ldots + \binom{n}{k_1}\right]$$

It follows that the inequality relationship as expressed by Eq. 4 is reversed if $\frac{1}{p}\,\frac{1-2\epsilon}{1-\epsilon} \geq 16$. Solve $\frac{1}{p}\,\frac{1-2\epsilon}{1-\epsilon} = 16$ for ϵ. From the definitions of p and ϵ, $p = \epsilon + 1/n$. Substituting this expression for p and rearranging, we obtain

$$\frac{1-2\epsilon}{1-\epsilon} = 16\left(\epsilon + \frac{1}{n}\right)$$

$$16\epsilon^2 - \left(18 - \frac{16}{n}\right)\epsilon + \left(1 - \frac{16}{n}\right) = 0$$

$$\epsilon = \frac{1}{16}\left(9 - \frac{8}{n}\right) \pm \frac{1}{16}\left(65 + \frac{112}{n} + \frac{64}{n^2}\right)^{1/2}$$

Only the negative sign yields a value within the range of interest. As n approaches infinity,

$$\epsilon \to \frac{1}{16}\left[9 - 65^{1/2}\right] \approx \frac{1}{17.06} > \frac{1}{18}$$

We conclude that for large n and $k_1 < n/18$ a change of more than 4 units in n may be required to produce a change in k_1.

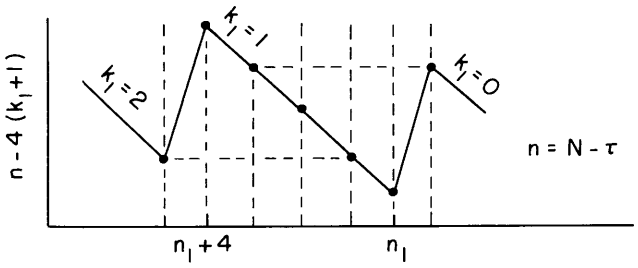

Fig. XV-3. Typical case in which the bound yields a greater value at $k_1 = 1$ than at $k_1 = 0$.

d. Simplified Expression of Sphere-Packing Bound for Alphabets of Practical Size

We have shown that the sphere-packing bound has its greatest value for a small value of k_1; specifically, the maximum value occurs at a value $k_1 < n/10$. The calculation of a bounding value can be greatly simplified by using the largest value of the expression for $k_1 = 0$; that is, by using Eqs. 5 and 6.

We shall now show that, for practical alphabet sizes, this is the greatest value of the bound for all k_1. The proof will be carried out by showing that (a) the bound can have a greater value for $k_1 = j + 1$ than for $k_1 = j$ only for excessively large M when $j = 0$; and (b) even larger values of M are required when $j > 0$.

(i) Minimum value of n [or M] for which the bound is greater at $k_1 = 1$ than at $k_1 = 0$

In order for the bound, $n - 4(k_1 + 1)$, to have a greater value at $k_1 = 1$ than at $k_1 = 0$, k_1 must remain fixed at $k_1 = 1$ while n changes four (or more) units. A typical situation of interest is shown in Fig. XV-3. Let n_1 be the smallest integer satisfying the expression

$$\frac{2^{n-1}}{M} \geq 1 + n$$

For convenience in notation, let $\phi[k_1 = j]$ represent the maximum value attained by the function $n - 4(k_1 + 1)$ for $k_1 = j$. To satisfy the condition postulated, $\phi[k_1 = 1] > \phi[k_1 = 0]$, it is required that

$$\frac{2^{(n_1+4)-1}}{M} < 1 + (n_1 + 4) + \frac{(n_1 + 4)(n_1 + 3)}{2}$$

Combining these two inequalities and solving for n_1 yields

$$\frac{2^{(n_1+4)-1}}{\frac{2^{n_1-1}}{1+n_1}} \leq \frac{2^{(n_1+4)-1}}{M} < 1 + (n_1 + 4) + \frac{(n_1 + 4)(n_1 + 3)}{2}$$

which reduces to

$$n_1^2 - 23n_1 - 10 > 0; \quad n_1 > 23.4; \quad \text{and} \quad n_1 \geq 24$$

Since n_1 is a function of M, it is more informative to express the bound in terms of M. If $\frac{2^{(n_1-1)-1}}{M} \geq 1 + (n_1 - 1)$, then $(n_1 - 1)$ is a point for which $k_1 = 1$. But it was assumed that n_1 was the smallest integer for which this was true. Therefore

$$\frac{2^{(n_1-1)-1}}{M} < 1 + (n_1 - 1) = n_1$$

$$M > \frac{2^{n_1-2}}{n_1} \geq \frac{2^{22}}{24} > 174,762$$

(ii) Proof that larger values of n are required for $\phi[k_1 = j + 1] > \phi[k_1 = j]$ when $j > 0$ than when $j = 0$.

Consider Fig. XV-4 for the general case. For some particular value of k_1, say $k_1 = j < n/4$, let n_o be the smallest integral value of n that will satisfy the inequality

$$\frac{2^{n-1}}{M} \geq 1 + n + \ldots + \binom{n}{j} \tag{18}$$

The value $\phi[k_1 = j]$ can be greater than the value $\phi[k_1 = j - 1]$ only if n can be increased four units (to $n_o + 4$) without increasing the value of k_1; that is,

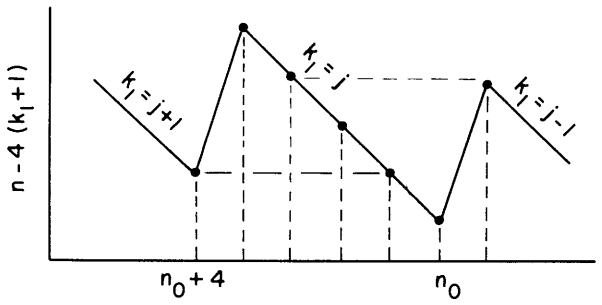

Fig. XV-4. Typical behavior of the bound for the range in which it increases with k_1.

$$\frac{2^{(n_o+4)-1}}{M} < 1 + (n_o + 4) + \ldots + \binom{n_o+4}{j+1} \tag{19}$$

It is not evident that this inequality can be satisfied in all cases for n_o as defined by Eq. 18. Indeed, previous results show that for this inequality to be satisfied, it is necessary that $j < n_o/10$. However, we are not interested here in the range for which Eq. 19 cannot be satisfied, for in that case $\phi[k_1 = j]$ cannot be greater than $\phi[k_1 = j - 1]$.

Before proceeding with the proof that the value of M that is required to make $\phi[k_1 = j + 1] > \phi[k_1 = j]$ is larger for $j > 0$ than for $j = 0$, it is well to verify the fact that if n_o is the smallest integer satisfying Eq. 18, another term, $\binom{n_o}{j+1}$, cannot be added without rendering the inequality invalid. Start with

$$\frac{2^{n_o-1}}{M} \geq 1 + n_o + \ldots + \binom{n_o}{j}$$

where n_o is the smallest integer satisfying this expression. Then

$$\frac{2^{(n_o-1)-1}}{M} < 1 + (n_o - 1) + \ldots + \binom{n_o-1}{j}$$

or

$$\frac{2^{n_o-1}}{M} < 2\left[1 + (n_o - 1) + \ldots + \binom{n_o-1}{j}\right] \tag{20}$$

But the ratios of i^{th} terms in the following series reveal that

$$1 + (n_o - 1) + \ldots + \binom{n_o-1}{j} < 1 + n_o + \ldots + \binom{n_o}{j} \quad \text{for} \quad j \geq 1$$

and

$$1 + (n_o - 1) + \ldots + \binom{n_o-1}{j} > \frac{1}{2}\left[1 + n_o + \ldots + \binom{n_o}{j}\right] \quad \text{for } j < \frac{n_o}{2}$$

For $j < n_o/4$, from Eq. 13, we have

$$\binom{n_o}{j+1} > 3\binom{n_o}{j} > 2\sum_{i=0}^{j}\binom{n_o}{i}$$

Then

$$1 + n_o + \ldots + \binom{n_o}{j} + \binom{n_o}{j+1} > 3\left[1 + n_o + \ldots + \binom{n_o}{j}\right]$$

In order for

$$\frac{2^{n_o-1}}{M} \geq 1 + n_o + \ldots + \binom{n_o}{j} + \binom{n_o}{j+1}$$

to be valid, it would be necessary that

$$\frac{2^{n_o-1}}{M} > 3\left[1 + n_o + \ldots + \binom{n_o}{j}\right]$$

but Eq. 20 shows that this is not true if n_o has the value assumed. Now, having established the fact that

$$\frac{2^{n_o-1}}{M} < 1 + n_o + \ldots + \binom{n_o}{j} + \binom{n_o}{j+1} \tag{21}$$

we shall proceed with the proof.

If there is some integer n for which

$$\frac{2^{n-1}}{M} \geq 1 + n + \ldots + \binom{n}{j} + \binom{n}{j+1} \tag{22}$$

let n_1 be the smallest such integer. Using the fact that

$$\frac{\binom{n}{j}}{\binom{n-1}{j}} = \frac{n}{n-j} < 2, \quad \text{for } j < \frac{n}{2}$$

we observe that, as n decreases, the left-hand side of Eq. 22 decreases faster than the right-hand side. We know from Eq. 21 that Eq. 22 is not satisfied for $n_1 = n_o$; therefore, it certainly cannot be satisfied for $n_1 < n_o$. It follows that $n_1 > n_o$, and that there is no value of k_1 that gives a smaller value of n_o than $k_1 = 0$.

Therefore, for $M < 174,762$ the function $n - 4(k_1 + 1)$ has its greatest value at $k_1 = 0$, and the bound reduces to Eqs. 5 and 6.

5. Proof that for Large M the Sphere-Packing Bound is Tighter than the log M Bound

It is of interest to compare the bound obtained by the sphere-packing argument, expressed by Eqs. 3 and 5, with the bound obtained by the point-space argument, expressed by Eq. 2. We wish to show that for large alphabets, the sphere-packing bound is tighter than the log M bound. It is sufficient to show that the sphere-packing bound

gives a larger value than the log M bound for one value of k_1, namely, for $k_1 = 0$. In this case, the sphere-packing bound is given by Eqs. 5 and 6. Then, for $k_1 = 0$ we have

$$1 \leq \frac{2^{n-1}}{M} < 1 + n$$

where n is the largest integer satisfying the inequality. It follows that

$$\frac{2^{(n+1)-1}}{M} \geq 1 + (n+1) = n + 2$$

or, after dividing through by 2, that

$$\frac{2^{n-1}}{M} \geq \frac{n+2}{2} = \frac{n}{2} + 1 \tag{23}$$

Let

$$\frac{2^{n-1}}{M} = 1 + n - \delta \qquad \delta > 0 \tag{24}$$

Combining Eqs. 23 and 24, we have

$$1 + n - \delta \geq \frac{n}{2} + 1$$

$$n - \delta \geq \frac{n}{2}$$

$$\delta \leq \frac{n}{2}$$

We wish to show that for n large, which corresponds to large M from Eq. 6, Eq. 5 gives a larger value than Eq. 2; that is, $n - 4 > \log M + \epsilon$, with $0 \leq \epsilon < 1$. Taking the logarithm of Eq. 24 yields $n - 1 - \log (1 + n - \delta) = \log M$. When we substitute this quantity for log M, the inequality in question becomes $n - 4 > n - [1 + \log (1 + n - \delta) - \epsilon]$. This inequality holds if

$$1 - \epsilon + \log (1 + n - \delta) > 4$$

or

$$\log (1 + n - \delta) > 3 + \epsilon,$$

or

$$n - \delta > 2^{3+\epsilon} - 1 \begin{cases} < 15 \\ \geq 7 \end{cases}$$

Since $n - \delta \geq \frac{n}{2}$, the inequality definitely holds for $n \geq 30$. Q.E.D.

G. E. Mongold, Jr.

References

1. R. W. Hamming, Error detecting and error correcting codes, Bell System Tech. J. 29, 147-160 (1950).

2. R. M. Fano, On matched-filter detection in the presence of multipath propagation, Memorandum, Research Laboratory of Electronics, M.I.T., 1956 (unpublished).

3. R. Price and P. E. Green, Jr., A communication technique for multipath channels, Proc. IRE 46, 555-570 (1958).

4. M. Plotkin, Binary codes with specified minimum distance, University of Pennsylvania, Moore School, Research Division Report 51-20, 1951.