#2

ERROR BOUNDS FOR PARALLEL COMMUNICATION CHANNELS

PAUL M. EBERT

Loan Copy Only

TECHNICAL REPORT 448

AUGUST 1, 1966

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
RESEARCH LABORATORY OF ELECTRONICS
CAMBRIDGE, MASSACHUSETTS

The Research Laboratory of Electronics is an interdepartmental laboratory in which faculty members and graduate students from numerous academic departments conduct research.

The research reported in this document was made possible in part by support extended the Massachusetts Institute of Technology, Research Laboratory of Electronics, by the JOINT SERVICES ELECTRONICS PROGRAMS (U.S. Army, U.S. Navy, and U.S. Air Force) under Contract No. DA36-039-AMC-03200(E); additional support was received from the National Science Foundation (Grant GP-2495), the National Institutes of Health (Grant MH-04737-05), and the National Aeronautics and Space Administration (Grants NsG-334 and NsG-496).

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

RESEARCH LABORATORY OF ELECTRONICS

Technical Report 448 August 1, 1966

ERROR BOUNDS FOR PARALLEL COMMUNICATION CHANNELS

Paul M. Ebert

Submitted to the Department of Electrical Engineering, M.I.T. August 10, 1965, in partial fulfillment of the requirements for the degree of Doctor of Science.

(Manuscript received December 21, 1965)

Abstract

This report is concerned with the extension of known bounds on the achievable probability of error with block coding to several types of paralleled channel models.

One such model is that of non-white additive Gaussian noise. We are able to obtain upper and lower bounds on the exponent of the probability of error with an average power constraint on the transmitted signals. The upper and lower bounds agree at zero rate and for rates between a certain R_{crit} and the capacity of the channel. The surprising result is that the appropriate bandwidth used for transmission depends only on the desired rate and not on the power or exponent desired over the range wherein the upper and lower bounds agree.

We also consider the problem of several channels in parallel with the option of using separate coders and decoders on the parallel channels. We find that there are some cases in which there is a saving in coding and decoding equipment by coding for the parallel channels separately. We determine the asymptotic ratio of the optimum blocklength for the parallel channels and analyze one specific coding scheme to determine the effect of rate and power distribution among the parallel channels.

TABLE OF CONTENTS

I. INTRODUCTION

The basic task of the communication engineer is to design systems to transmit information from one point to another, and the way he goes about designing the system depends largely on the nature of the information and the transmission channels available. The output of a physical channel is never an exact reproduction of the signal that was transmitted; there is some distortion introduced by the channel. The system designer must search for a way to minimize the effect of this distortion on the reliability of transmission. This is done through some sort of processing at the transmitter and receiver, where the effectiveness of the processing is reflected in the resulting error in information transmission, as distinct from the channel distortion.

In order to speak quantitatively about the error in the processed output it is necessary to define some way to measure the error. The type of measure that is used will depend largely on the form of the information to be transmitted. If it is digital information one usually speaks of the probability of error, which is defined as the probability that the processed output is incorrect. When the information to be transmitted takes on a continuum of values we know that we cannot possibly hope to reproduce it without some small error, and hence some measure other than P_e is needed. In some cases one uses mean-square error.

$$\overline{[\hat{s}(t) - s(t)]^2},$$

where $\hat{s}(t)$ is the correct output. The mean-square error is not the only measure that can be applied to continuous signals, although it is probably used more often than it should be because it is so easy to work with. In speech reproduction, for example, mean-square error has little correspondence to any subject measure of quality.

Shannon[22] has considered the problem of a discrete representation of a continuous source. For a given continuous source and any reasonable measure of distortion, he defined a certain rate corresponding to each value of distortion, D. He found that the continuous source could be transmitted over any channel having a capacity larger than R with a resulting distortion equal to or less than D. Conversely, he showed that the source could not be transmitted over a channel having a capacity less than R without the resulting distortion being larger than D.

We can use Shannon's result to show than any continuous source can be represented by a discrete source of rate R, such that the continuous signal can be reconstructed from the discrete signal with a distortion equal to or less than D. To show this, we take as the channel in Shannon's results an error-free discrete channel with capacity R. The input (or output) of this channel is the discrete representation that we desire.

For the purpose of analysis, any continuous source can be represented as a discrete source, with a certain distortion D. This source is then transmitted over the channel with an arbitrarily small P_e, and the continuous signal reconstructed at the receiver with a resulting distortion only slightly larger than D. The problem of transmitting continuous information can therefore be broken down into two parts: the representation of the continuous source as a discrete source with an implicit distortion D, and the transmission of the discrete information. In addition to the generality of the discrete representation of continuous signals there is a growing trend in the communication industry to convert continuous sources into discrete sources by sampling and quantizing, primarily to facilitate multiplexing. In any event, the discrete source is an important one in its own right, because of the recent increase in digital data transmission. For these reasons, we shall consider only discrete sources in this report.

The case of the discrete source was considered by Shannon.[17] He showed that as long as the rate was less than the capacity of the channel one could obtain an over-all P_e as close to zero as one desired by coding and decoding over a sufficiently long block of channel digits. The capacity of the channel is defined as the maximum mutual information between the input and output of the channel per digit, and the rate, R, of the source is the entropy of its output.

The P_e which Shannon was concerned with was the probability that at least one letter in a block of source letters was decoded incorrectly, rather than the probability that any single source letter was incorrect. Therefore the block P_e is an upper bound for the individual P_e, since a block is considered to be correct only if all of the letters in it are correct. When we refer to P_e for block coding we shall always mean the block P_e.

For rates above capacity Shannon showed that one could not make P_e small, and Wolfowitz[23] showed that P_e actually approached 1 as the blocklength was increased.

Below capacity, Feinstein[6] showed that P_e was upper-bounded by an exponentially decreasing function of blocklength. Fano[5] developed a sphere-packing argument to show that P_e was also lower-bounded by an exponentially decreasing function. For this reason, the reliability function is defined as the limit of the exponential part of P_e,

$$E(R) \equiv \lim_{N\to\infty} \sup \frac{-\ln P_e}{N}, \tag{1}$$

where N is the blocklength. The usefulness of E(R) lies in the implication of (1)

$$P_e \leqslant e^{-N[E(R)-\epsilon]}. \tag{2}$$

For every $\epsilon > 0$ there is a sequence of N approaching ∞ for which (2) is met. Upper and lower bounds on E(R) have been calculated by Fano,[5] and it was found that they agreed for rates larger than a certain rate called R_{crit}.

Gallager[8] has produced a simple derivation of the upper bound on P_e and improved this bound at low rates by an expurgation technique. He has given a rigorous proof[21] of the sphere-packing bound and Berlekamp[1] has found that the zero-rate lower bound is exponentially the same as the upper bound. Shannon[21] and Gallager found a straight-line bound to connect the sphere-packing bound to the zero-rate bound.

The reliability function is not limited to discrete channels. One can include amplitude-continuous, time-discrete channels by approximating the continuous channel by a quantized discrete channel. If the E(R) of the quantized channel converges as the quantization is made finer, that limit is called the E(R) of the amplitude-continuous channel. Rice,[16] Kelly,[13] and Ziv[27] have considered the amplitude-continuous channel disturbed by Gaussian noise. They showed that one could obtain an exponential P_e by using signals chosen from a Gaussian ensemble.

Shannon[19] derived upper and lower bounds on E(R) with additive Gaussian noise and an average constraint that agreed above R_{crit}. In order to do this, he constrained all of his signals to have the same energy. Gallager[8] considered the same problem but constrained the signals to have energy within δ of the average energy. He got the same upper-bound exponent as Shannon, but was able to get a better bound at low rates by an expurgation technique. Shannon found that the upper- and lower-bound exponents agreed at zero rate, and Wyner[26] has found an improved bound for small rates.

Shannon[19] observed that, by the sampling theorem, a time-continuous bandlimited channel with additive white Gaussian noise is equivalent to the time-discrete Gaussian channel just mentioned. This concept can be made rigorous by the use of the Karhunen-Loève theorem, as is done in Section I. The Karhunen-Loève theorem can also be used to consider non-white Gaussian noise. This was done by Holsinger.[11] He introduced the power constraint by using a multidimensional Gaussian signal with a constraint on the sum of the variances. He derived an upper-bound exponent that was only slightly inferior to Gallager's for the white noise bandlimited case.

The work done for the continuous-time channel indicates that P_e can be made exponential in the time duration, T, of the transmitted code words; in other words, T takes the place of N in relating E(R) to P_e. Thus in this case we define

$$E(R) \equiv \lim_{T\to\infty} \frac{-\ln P_e}{T}.$$

The tightest known bounds generally fall into one of 5 important classes; two upper bounds and three lower bounds as shown in Fig. 1 and tabulated in Table 1. The upper bounds are the random coding bound and the expurgated bound which together are the tightest known upper bounds. The three lower bounds are the sphere-packing bound, the minimum-distance bound, and the straight-line bound. Together these are the tightest known lower bounds.

Here we are primarily interested in the problem of parallel communication channels. By parallel channels we mean a communication system or model (similar to that shown in Fig. 2) where the distortion introduced by each channel is independent of the signal and the distortion in all of the other channels. Gallager[8] has considered this problem when the channels are fixed and the same blocklength is used on all of the parallel channels, i.e., input letters are chosen from the product alphabet of all channels.

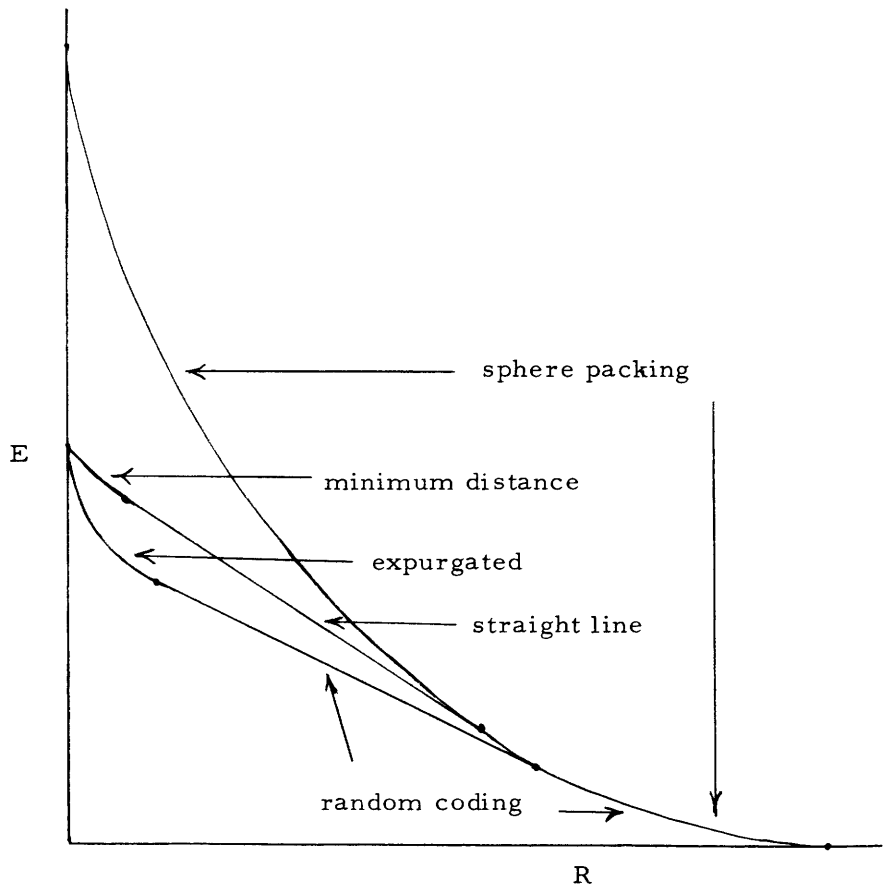


Fig. 1. Typical E(R) bounds.

Table 1. Five classes of bounds and references to presentations.

Channel	Discrete Constant	Time-Discrete Gaussian Noise Power Constraint
Upper Bounds Random-Coding Bound	Shannon[19] Fano[5] Gallager[8]	Shannon[20]
Expurgated Bound	Gallager[8]	Gallager[8]
Lower Bounds Sphere-Packing	Fano[5] Gallager[21]	Shannon[20]
Minimum-Distance	Elias[4] (BSC) Berlekamp[1] (zero rate)	Shannon[20] (zero rate) Wyner[26]
Straight-Line	Shannon and Gallager[21]	–

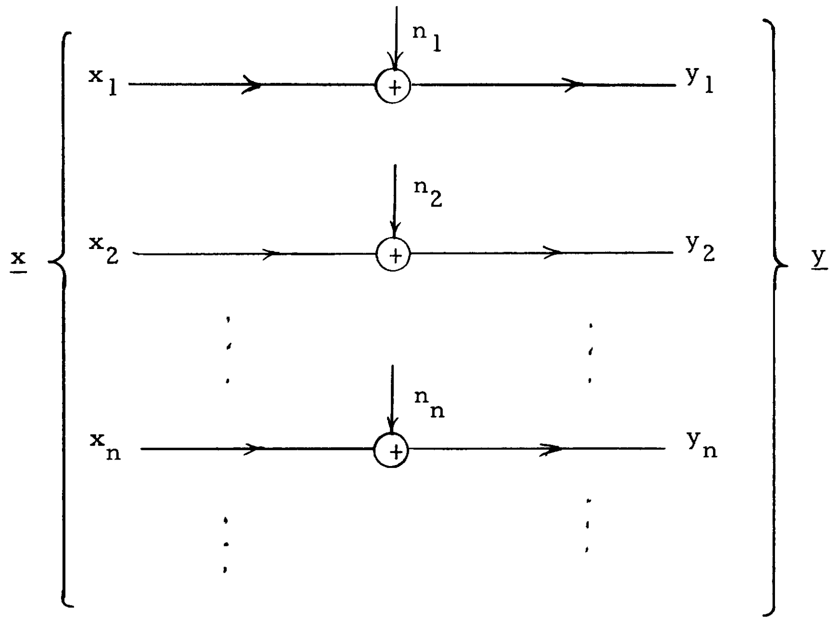


Fig. 2. Model to be analyzed.

We are interested in problems with an additional amount of freedom. In Sections I and II, we analyze the combination of parallel channels, each with additive Gaussian noise. In this case the crucial problem is the distribution of the signal power among the parallel channels. By the Karhunen-Loève theorem the time-continuous channel with additive Gaussian noise and an average power constraint can be analyzed in this class of parallel channels. We are able to find the five upper and lower bounds already mentioned for this channel. The upper bounds are given in Eqs. 20, 21, and 30, and the lower bounds in Eqs. 47, 61, 62, and 64.

The function E(R) gives the relationship between the blocklength and P_e, but it tells nothing about how to implement such a coder and decoder. For practical purposes, the amount of equipment needed to code and decode is of paramount importance. As long as one has only a single channel, one must choose a sufficiently large blocklength to meet the desired P_e and then must build a coder-decoder to operate at that blocklength. If one has several channels in parallel and is willing to use different blocklengths on the channels, one must have some relation between blocklength and cost before any analysis is possible. For this purpose, we introduce a complexity function that is a function of the channel, the coding scheme, the rate, and the blocklength. It relates the complexity, or cost, in logical operations per second to all of the variables listed above. We can then vary the rates and blocklengths on the parallel channels, subject to constant total rate and total complexity. We find that there are many cases in which there is a small advantage in using different blocklengths on parallel channels. It is also possible that one does not have the opportunity to use composite coding. For example, if one is working with networks of communication channels, the intermediate terminals are not able to do any decoding unless they receive the entire block. On the other hand, the intermediate terminals cannot receive entire blocks unless separate coding is used on each channel in the network.

We have considered in detail one particular coding and decoding scheme for which the complexity function is known. This scheme has two stages of coding, an inner coder with a maximum-likelihood decoder, and an outer coder using a Reed-Solomon code. The maximum-likelihood inner coder-decoder is only practical in a limited number of situations, but the results of the analysis may be indicative of what may be expected from other schemes.

We have considered the problem of power distribution with fixed blocklength, and the problem of rate and blocklength distribution with fixed power. It is possible that we may have to choose both of these distributions at once. The formulation of this problem does not lead to an analytic solution, bit it appears that the solution is not significantly different from that without blocklength freedom. This is to say that composite coding over all the parallel is a fair first-order approximation, insofar as P_e is concerned, to separate coding with the optimum rate distribution.

II. CHANNELS WITH ADDITIVE GAUSSIAN NOISE

We are now concerned with channels with additive Gaussian noise. These can be time-discrete channels or continuous channels with colored noise. By suitable manipulation we can even analyze channels that filter the signal before the noise is added. The entire analysis is made possible by the representation of signal and noise by an orthogonal expansion to which some recent theorems[8, 21] on error bounds can be applied.

We shall begin by considering a channel that has as the received signal the transmitted noise signal plus stationary Gaussian noise with autocorrelation function $R(\tau)$. Suppose one is interested in the properties of the channel under the conditions that the transmitted signal be of duration T seconds and that the receiver make its decision about what was transmitted on the basis of an observation of the T-second interval. Then a very convenient representation of the noise in the channel is given by the Karhunen-Loève theorem.[2] This theorem states that given a Gaussian noise process with autocorrelation function $R(\tau)$ the noise can be represented, in the mean, by the infinite sum

$$n(t) = \sum_{i=1}^{\infty} n_i \phi_i(t),$$

where the $\phi_i(t)$ are the eigenfunctions of the integral equation

$$\int_0^T R(t-\tau)\ \phi_i(\tau)\ d\tau = N_i \phi_i(t); \qquad 0 \leq t \leq T$$

and the coefficients n_i are Gaussian, independent, and have variance N_i. The eigenfunctions being orthonormal also make a convenient basis for the signal. In this representation there are two problems which must be eliminated if one is to get anything other than trivial solutions. First, the set of $\phi_i(t)$ should be complete in some sense. If it is possible to send signals which have finite power and are orthogonal to the noise, these are clearly the signals to use. Thus for all interesting problems $R(\tau)$ is such that the set $\phi_i(t)$ is complete over square integrable functions (that is, L_2 functions). Second, we would like to consider cases for which $R(\tau)$ is not in L_2, as required by the Karhunen-Loève theorem. It turns out that if $R(\tau)$ is in L_2, some of the N_i are arbitrarily small (that is, 0 is a limit point of the N_i). Therefore the corresponding eigenfunctions are ideal signals. There are various ways out of the difficulty and the one used here is probably not as powerful as some others, but is easily visualized and analyzed. One merely observes that if $R(\tau)$ consists of an impulse minus an $R'(\tau)$ in L_2, the associated integral equation has the same eigenfunctions as $R'(\tau)$ but now the eigenvalues are $N_o - N_i'$, where N_o is the magnitude of the impulse, and N_i' is an eigenvalue of $R'(\tau)$. Now some of the N_i are not arbitrarily small but instead approach N_o. Since in any real problem all eigenvalues, being variances, must be positive, N_o must be larger than the largest eigenvalue of $R'(\tau)$. Now one only requires that $R'(\tau) = N_o\mu_o(\tau) - R(\tau)$ be in L_2. Another reason for using this approach can be seen from intuitive reasoning. One would expect that a good signaling scheme would concentrate most of its power where the noise is weakest. Therefore any representation that allows noise power to go to zero even in remote parts of the spectrum will be self-defeating. Since the least noisy part of the noise spectrum is the part most intimately involved in the analysis, it is a good idea to have a simple expression for it.

Now that the noise and signal can be broken up into orthogonal parts and represented by a discrete set of numbers, we can represent the channel as a time-discrete memoryless channel. For any time interval T we have an infinite set of eigenfunctions that can be used as the basis of the signal, and the noise in each of the eigenfunctions is independent.

$$n(t) = \sum_{n=1}^{\infty} n_n \phi_n(t),$$

$$x(t) = \sum_{n=1}^{\infty} x_n \phi_n(t).$$

The received signal y(t) is the sum of them, or

$$y(t) = \sum_{n=1}^{\infty} (n_n + x_n)\, \phi_n(t).$$

Thus far, we have reduced the channel to a set of time-discrete channels each with independent Gaussian noise and each operating once every T seconds, one for each eigenfunction (see Fig. 2). The noises are not independent from one T-second interval to the next, but we do not need this.

Because of the parallel channel representation we have an implicit blocklength of one. Consequently, the parameters E and R will differ by a factor of T from those already defined; in other words,

$$R = \ln M$$

$$E = -\ln P_e$$

$$S = TP.$$

There are other ways of dealing with colored Gaussian noise and frequency constraints on the signals, but all of them eventually reduce the channel to a set of parallel Gaussian noise channels. Our results apply equally well to any of these cases.

Before going on to the bounds on the error probability we shall point out the other channels that reduce to this representation. Any number of time-discrete channels in parallel with additive Gaussian noise can be represented by making T an integral

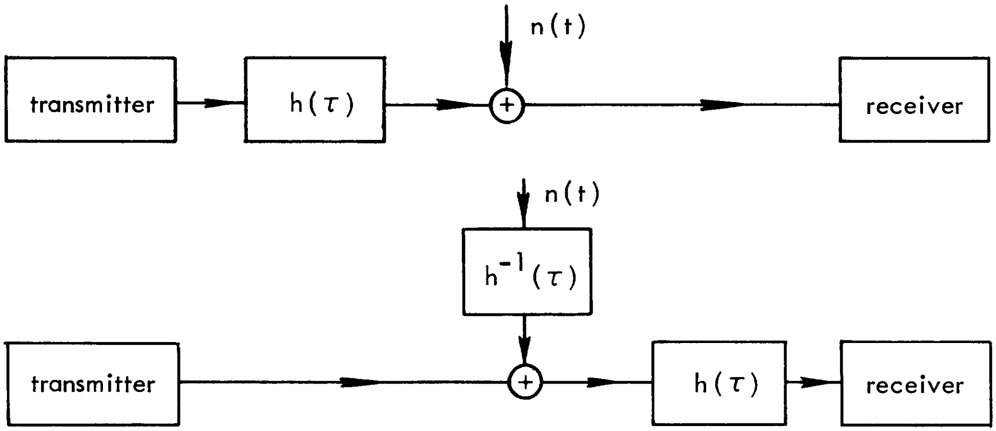


Fig. 3. Conversion of filtered channel to colored noise channel.

multiple of the period of the channels. The multiplicative integer is known as the block-length in the standard approach. This is a more general representation of time-discrete channels than the one considered by Shannon,[20] since it allows the parallel channels to have different noise levels.

The other case that can be reduced to this representation is that shown in Fig. 3. This can be redrawn as in Fig. 3 and one has the original problem, except that now there is a filter before the receiver. The filter does not change the problem because any part of the signal that will not go through the filter will not go through the channel, and consequently will not be used by an optimum coder.

2.1. UPPER BOUND TO THE ATTAINABLE PROBABILITY OF ERROR

Gallager[8] has considered the problem of coding for the general noisy channel in which there is a probability density of output signals, given any input signal, $P(\underline{y}/\underline{x})$.

In order to obtain a $P(\underline{y}/\underline{x})$ for our model, we need to limit the vectors $\underline{x}$ and $\underline{y}$ to a finite dimensionality. This is also necessary for certain theorems that we shall use later. Therefore we shall solve the finite (N) dimensional problem and then let $N \to \infty$. It turns out that sometimes the codes only use a finite dimensional $\underline{x}$. When $\underline{x}$ is limited to a finite dimensionality we can ignore all coordinates of $\underline{y}$ which result from noise only. They are independent of the signal and the other noise; thus they cannot aid in the decoding.

The bound obtained is a random coding bound and operates as follows. The transmitter has a set of M code words each of which are chosen independently and randomly from the input space $\underline{x}$ according to a probability distribution $P(\underline{x})$. This defines an ensemble of codes; hence the name random code. Henceforth we shall write $P(\underline{x})$ as $\underline{P}$ for notational simplicity but it should be remembered that $\underline{P}$ is a function of $\underline{x}$. One of the M code words is selected for transmission by the source.

The receiver, knowing what all M possible code words are, lists the L most likely candidates based on the received waveform $\underline{(y)}$. We define the probability that the transmitted code word is not on the list as P_e. In Appendix C we outline a proof that P_e averaged over the ensemble of codes is bounded by

$$\overline{P}_e \leq \exp -[E_o(\rho,\underline{P})-\rho R] \tag{3}$$

for any $0 \leq \rho \leq L$, where

$$R = \ln \frac{M}{L}$$

and

$$E_o(\rho,\underline{P}) = -\ln \int_{\underline{y}} \left(\int_{\underline{x}} \underline{P} p(\underline{y}/\underline{x})^{\frac{1}{1+\rho}} d\underline{x} \right)^{1+\rho} d\underline{y} \tag{4}$$

Since $\overline{P}_e$ is the average P_e over the ensemble, there must exist some code in this ensemble with $P_e \leq \overline{P}_e$.

There is no particular reason for making $L \neq 1$, except that it brings in no added difficulties and adds a little insight on how much the bound on P_e can be improved by making L larger than 1. In our model we have

$$P(\underline{y}/\underline{x}) = \prod_{n=1}^{N} P(y_n/x_n) = \prod_{n=1}^{N} \frac{\exp -\frac{(y_n-x_n)^2}{2N_n}}{\sqrt{2\pi N_n}}. \tag{5}$$

The integrals in (4) are carried out over the entire input and output spaces.

In order to introduce an average energy constraint on $\underline{x}$, we shall use a $\underline{P}$ which is zero for $|\underline{x}|^2$ greater than S.

In order to get a strong bound on P_e, we need to eliminate many of the signals with small energy and thus use a $\underline{P}$ that is zero for $|\underline{x}|^2$ less than $S - \delta$, when δ is a small number to be chosen later. This is done by taking a multidimensional Gaussian probability density

$$P_g(\underline{x}) = \prod_{n=1}^{N} \frac{\exp -\frac{x_n^2}{2Q_n}}{\sqrt{2\pi Q_n}},$$

where the variables Q_n will be determined later, then confining $\underline{x}$ to a shell by multiplying $P_g(\underline{x})$ by $\Phi(x)$, and renormalizing

$$\Phi(\underline{x}) = \begin{cases} 1; & -\delta \leq \sum_{n=1}^{N} x_n^2 - S \leq 0 \\ 0; & \text{otherwise} \end{cases}$$

Therefore we have

$$\underline{P} = \frac{1}{q} P_g(\underline{x})\ \Phi(\underline{x}), \tag{6}$$

where

$$q = \int_{\underline{x}} P_g(\underline{x})\ \Phi(\underline{x})\ d\underline{x}.$$

We have now obtained the shell-constrained $\underline{P}$, but it is difficult to evaluate the integral of (4). We observe that if we have a function

$$w(\underline{x}) \geq \Phi(\underline{x}) \tag{7}$$

for all $\underline{x}$ in the input space we can substitute $\frac{1}{q} w(\underline{x})\ P_g(\underline{x})$ for $\underline{P}$ in (4) and still have a bound on P_e. We therefore choose $w(\underline{x})$ to be factorable as $p_g(\underline{x})$ is and to have a Gaussian shape for ease of integration.

$$w(\underline{x}) = \exp\left[r \sum_{n=1}^{N} x_n^2 - rS + \delta r\right], \tag{8}$$

in which the quantity r is an arbitrary non-negative number that will be specified later. Equation 7 is met for any $\underline{x}$, since $w(\underline{x}) \geq 0$, and for those $\underline{x}$ for which $\Phi(\underline{x}) = 1$,

$$\sum_{n=1}^{N} x_n^2 \geq S - \delta.$$

Thus the exponent in (8) is non-negative, and $w(x) \geq 1$. Consequently, we can substitute Eqs. 6 and 7 in Eq. 4 to get

$$E_o(\rho, \underline{P}) \geq -\ln\left(\frac{e^{-Sr+\delta r}}{q}\right)^{1+\rho} \prod_{n=1}^{N} \int_{y_n} \left[\int_{x_n} \frac{\exp\left(-\frac{x_n^2}{2Q_n} + rx_n^2 - \frac{(y_n-x_n)^2}{2N_n(1+\rho)}\right)}{\sqrt{2\pi Q_n}\,\left(\sqrt{2\pi N_n}\right)^{\frac{1}{1+\rho}}}\, dx_n\right]^{1+\rho} dy_n.$$

Upon completing the square in x_n, this becomes

$$E_o(\rho, \underline{P}) \geq (1+\rho) \ln q + (1+\rho)(S-\delta)r$$

$$- \sum_{n=1}^{N} \ln \int_{y_n} \left[\sqrt{\frac{(1+\rho)N_n^{\frac{\rho}{1+\rho}}}{[Q_n+(1+\rho)N_n(1-2rQ_n)](2\pi)^{\frac{1}{1+\rho}}}}\ \exp - \frac{y_n^2(1-2rQ_n)}{2[Q_n+(1+\rho)N_n(1-2rQ_n)]}\right]^{1+\rho} dy_n,$$

and completing the square in y_n, we get

$$E_o(\rho, \underline{P}) \geq (1+\rho) \ln q + (1+\rho)(S-\delta)r - \sum_{n=1}^{N} \ln \sqrt{\frac{N_n^{\rho}}{(1-2rQ_n)\left[\frac{Q_n}{1+\rho} + N_n(1-2rQ_n)\right]^{\rho}}}. \tag{9}$$

At this point it is best to examine the quantity $(1+\rho)(\ln q - \delta r)$. It is necessary that this quantity grow less than linearly with T so that when the exponent is divided by T the effect of this term will vanish. There are several ways that this can be done, but a sufficient condition is that the probability density of the function $\sum_{n=1}^{N} x_n^2 \equiv |\underline{x}|^2$ have its mean within the range $S - \delta$ to S, when $\underline{x}$ is distributed according to $p_g(\underline{x})$. This is accomplished by letting

$$\sum_{n=1}^{N} Q_n = S. \tag{10}$$

If δ is fixed at an appropriate value it is shown in Appendix B that q decreases only as $1/\sqrt{T}$.

By substituting (10) in (9), and (9) in (3) we can write

$$P_e \leq B \exp\left(\rho R - \sum_{n=1}^{N} (1+\rho)Q_n r + \frac{1}{2} \ln (1-2rQ_n) + \frac{\rho}{2} \ln \left[1 - 2rQ_n + \frac{Q_n}{(1+\rho)N_n}\right]\right),$$

where $B = \left(\frac{e^{\delta}}{q}\right)^{1+\rho}$. The problem has now been reduced to minimizing the quantity above, subject to the constraints

$$\sum_{n=1}^{N} Q_n = S, \qquad Q_n \geq 0, \qquad r \geq 0, \qquad 0 \leq \rho \leq L.$$

The factor B will not be included in the minimization because it is hard to handle, and, as we have just pointed out, it does not contribute to the exponential part of P_e. First the minimization will be done with respect to r and Q_n; in this case we need maximize only

$$\sum_{n=1}^{N} \left[r(1+\rho) Q_n + \frac{1}{2} \ln (1-2rQ_n) + \frac{\rho}{2} \ln \left(1 - 2rQ_n + \frac{Q_n}{(1+\rho)N_n}\right)\right]. \tag{11}$$

We now introduce a new set of variables. Substitute β_n for rQ_n wherever it appears in (11). This puts Eq. 11 in a form to which the Kuhn-Tucker theorem[14] can be applied. When we maximize over the sets β_n and Q_n we are doing so over a larger space than allowed (since $\beta_n/Q_n = r$ for all n), but if the maximum turns out to fall within the allowed subset, then it is still the maximum solution. Thus we wish to maximize

$$F(\rho, Q_n, \beta_n) = \sum_{n=1}^{N} \left[(1+\rho)\beta_n + \frac{1}{2} \ln (1-2\beta_n) + \frac{\rho}{2} \ln \left(1 - 2\beta_n + \frac{Q_n}{(1+\rho)N_n}\right)\right].$$

The Kuhn-Tucker theorem states that a jointly concave function is maximized subject to the constraints

$$\beta_n \geq 0, \qquad Q_n \geq 0, \qquad \sum_{n=1}^{N} Q_n = S$$

if and only if

$$\frac{\partial F}{\partial Q_n} \leq A; \qquad \text{equality if } Q_n \neq 0$$

$$\frac{\partial F}{\partial \beta_n} \leq 0; \qquad \text{equality if } \beta_n \neq 0,$$

where A is chosen to meet the constraint on the sum of the Q_n. Taking these derivatives, we obtain

$$\frac{\rho}{2} \frac{\dfrac{1}{(1+\rho)N_n}}{\dfrac{Q_n}{(1+\rho)N_n} + 1 - 2\beta_n} \leq A; \qquad \text{for all } n \tag{12}$$

$$(1+\rho) + \frac{1}{2} \frac{-2}{1 - 2\beta_n} + \frac{\rho}{2} \frac{-2}{\dfrac{Q_n}{(1+\rho)N_n} + 1 - 2\beta_n} \leq 0; \qquad \text{for all } n. \tag{13}$$

First we note that if $Q_n = 0$, then by Eq. 13,

$$(1+\rho) \frac{-2\beta_n}{1 - 2\beta_n} \leq 0.$$

If $\beta_n \neq 0$, then we must have equality and $\beta_n = 0$; consequently, β_n must equal 0. Thus if $Q_n = 0$, then $\beta_n = 0$. On the other hand, if $\beta_n = 0$, (13) gives

$$(1+\rho) - 1 - \frac{\rho}{\dfrac{Q_n}{(1+\rho)N_n} + 1} \leq 0,$$

or

$$\frac{Q_n}{(1+\rho)N_n} \leq 0,$$

but since $(1+\rho)N_n > 0$, and $Q_n \geq 0$,

$$Q_n = 0.$$

Consequently, Q_n and β_n are either both zero or both nonzero.

Both Eqs. 12 and 13 then will be met with equality when $\beta_n \neq 0$. From Eq. 12 we have

$$\frac{\rho}{2} \frac{1}{\dfrac{Q_n}{(1+\rho)N_n} + 1 - 2\beta_n} = (1+\rho)N_n A.$$

Substituting this in (13), we have

$$1 + \rho - \frac{1}{1 - 2\beta_n} - 2(1+\rho)\, N_n A = 0,$$

or

$$\frac{1}{1 - 2\beta_n} = (1+\rho)(1-2N_n A). \tag{14}$$

Substituting this in (12), we get

$$Q_n = \frac{\rho}{2A} - \frac{N_n}{1 - 2AN_n} = \frac{1}{2A}\left(1 + \rho - \frac{1}{1 - 2AN_n}\right),$$

while from (14) we get

$$\beta_n = \frac{1}{2} - \frac{1}{2(1+\rho)(1-2AN_n)} = \frac{1}{2(1+\rho)}\left(1 + \rho - \frac{1}{1 - 2AN_n}\right).$$

Therefore

$$r = \frac{\beta_n}{Q_n} = \frac{A}{1 + \rho},$$

and maximizing over the larger set of variables β_n and Q_n yields a maximization to the original problem. From Eq. 12 we have

$$1 + \rho - \frac{1}{1 - 2\beta_n} - 2AN_n(1+\rho) \leq 0$$

or

$$\frac{1}{1 - 2\beta_n} \geq (1+\rho)(1-2AN_n); \quad \text{equality if } \beta_n \neq 0.$$

Because of the limitation $\beta_n \geq 0$, $\frac{1}{1-2\beta_n} \geq 1$, the equality can be met only when

$$(1+\rho)(1-2AN_n) \geq 1;$$

thus, for all $N_n \geq \frac{\rho}{2A(1+\rho)}$, $\beta_n = 0$, and $Q_n = 0$. If we call N_b the boundary value of N_n, $N_b = \frac{\rho}{2A(1+\rho)}$, we can say that for all $N_n \leq N_b$

$$Q_n = \frac{1}{2A}\left(1+\rho-\frac{1}{1-2AN_n}\right) = \frac{(1+\rho)^2 (N_b-N_n)}{1+\rho-\rho\frac{N_n}{N_b}}, \tag{15}$$

$$r = \frac{A}{1+\rho} = \frac{\rho}{2N_b(1+\rho)^2},$$

and for all $N_n \geq N_b$,

$$Q_n = 0.$$

$$S = \sum_{n=1}^{N} Q_n = \sum_{N_n \leq N_b} \frac{(1+\rho)^2 (N_b-N_n)}{1+\rho-\rho\frac{N_n}{N_b}}, \tag{16}$$

with N_b determined by S according to Eq. 16.

For notational convenience, we shall write the sum over all n such that $N_n \leq N_b$ as the sum over the set n_o.

Using (15) and (16), we can now write

$$P_e \leq B \exp\left[-\frac{\rho S}{2N_b(1+\rho)} + \sum_{n_o} \frac{1}{2}\ln\left(1+\rho-\rho\frac{N_n}{N_b}\right) - \frac{\rho}{2}\sum_{n_o} \ln \frac{N_b+\rho(N_b-N_n)}{N_n\left(1+\rho-\rho\frac{N_n}{N_b}\right)} + \rho R\right].$$

The exponential part will be minimized over ρ, for fixed R and S. The last term can be simplified to

$$\frac{\rho}{2}\sum_{n_o} \ln \frac{N_b\left(1+\rho-\rho\frac{N_n}{N_b}\right)}{N_n\left(1+\rho-\rho\frac{N_n}{N_b}\right)} = \frac{\rho}{2}\sum_{n_o} \ln \frac{N_b}{N_n},$$

thereby giving

$$P_e \leq B \exp -E(\rho, N_b S, R),$$

$$E(\rho, N_b, S, R) = \frac{S}{2(1+\rho)\, N_b} - \sum_{n_o} \ln\left(1 + \rho - \rho\frac{N_n}{N_b}\right) + \frac{\rho}{2}\sum_{n_o} \ln\frac{N_b}{N_n} - \rho R.$$

Since S is to be constant, we can use the expression for S (Eq. 16) as the defining relation between N_b and ρ. Then

$$\frac{dE}{d\rho} = \frac{\partial E}{\partial \rho} + \frac{\partial E}{\partial N_b}\frac{dN_b}{d\rho}.$$

Taking these partial derivatives, we have

$$\frac{\partial E}{\partial N_b} = \frac{-\rho S}{2(1+\rho)\, N_b^2} - \frac{1}{2}\sum_{n_o} \frac{\rho\frac{N_n}{N_b^2}}{1 + \rho - \rho\frac{N_n}{N_b}} + \frac{\rho}{2}\sum_{n_o}\frac{1}{N_b}$$

$$= \frac{-\rho S}{2(1+\rho)\, N_b^2} + \sum_{n_o} \frac{\rho}{2N_b^2}\, \frac{(1+\rho)(N_b - N_n)}{1 + \rho - \rho\frac{N_n}{N_b}}.$$

To be precise, we need another term in $\partial E/\partial N_b$ to account for variations in n_o with N_b. This term is zero, as can be seen by assuming that the summation is done over all n but that the argument is zero for $N_n > N_b$. Now when we take the derivative with respect to N_b, the zero terms contribute to nothing.

Using (16), we obtain

$$\frac{\partial E}{\partial N_b} = 0$$

$$\frac{\partial E}{\partial \rho} = \frac{S}{2(1+\rho)^2\, N_b} - \frac{1}{2}\sum_{n_o} \frac{1 - \frac{N_n}{N_b}}{1 + \rho - \rho\frac{N_n}{N_b}} + \frac{1}{2}\sum_{n_o} \ln\frac{N_b}{N_n} - R$$

$$= \frac{S}{2(1+\rho)^2\, N_b} - \frac{1}{2(1+\rho)^2\, N_b}\sum_{n_o} \frac{(1+\rho)^2 (N_b - N_n)}{1 + \rho - \rho\frac{N_n}{N_b}} + \frac{1}{2}\sum_{n_o} \ln\frac{N_b}{N_n} - R.$$

By using Eq. 16 again, this becomes

$$\frac{\partial E}{\partial \rho} = \frac{1}{2}\sum_{n_o} \ln\frac{N_b}{N_n} - R. \tag{17}$$

Thus when one sets $\frac{dE}{d\rho} = 0$ one obtains

$$R = \frac{1}{2} \sum_{n_o} \ln \frac{N_b}{N_n}. \tag{18}$$

Therefore

$$E = \frac{\rho S}{2(1+\rho) N_b} - \frac{1}{2} \sum_{n_o} \ln \left(1 + \rho - \rho \frac{N_n}{N_b}\right). \tag{19}$$

For a given R and S, N_b is determined from (18), ρ from (16), and E from (19). To show that Eq. 19 yields a maximum for E over ρ, we need only show that $\frac{dE}{d\rho}$ (Eq. 17) is positive for ρ less than the stationary point and negative for ρ greater than the stationary point. Since (17) is monotone in N_b and passes through 0 at N_b corresponding to the stationary point, we need only show that $\frac{dN_b}{d\rho} < 0$, where N_b and ρ are related by (16):

$$\frac{dN_b}{d\rho} = - \frac{\displaystyle\sum_{n_o} \frac{(N_b - N_n)\left(1 + \rho - \rho \frac{N_n}{N_b} + \frac{N_n}{N_b}\right)}{\left(1 + \rho - \rho \frac{N_n}{N_b}\right)^2}}{\displaystyle\sum_{n_o} \frac{(1+\rho)\left(1 + \rho\left[1 - \frac{N_n}{N_b}\right]^2\right)}{\left(1 + \rho - \rho \frac{N_n}{N_b}\right)^2}} < 0,$$

which proves that the stationary point is the maximum.

We now write (19), (18), and (16) in parametric form, these three relations being the derived bound.

$$E(N_b, \rho) = \frac{\rho S}{2(1+\rho) N_b} - \frac{1}{2} \sum_{n_o} \ln \left(1 + \rho - \rho \frac{N_n}{N_b}\right) \tag{20a}$$

$$R(N_b, \rho) = \frac{1}{2} \sum_{n_o} \ln \frac{N_b}{N_n} \tag{20b}$$

$$S(N_b, \rho) = \sum_{n_o} \frac{(1+\rho)^2 (N_b - N_n)}{1 + \rho - \rho \frac{N_n}{N_b}}. \tag{20c}$$

There is a restriction in Eq. 3 that $0 \leq \rho \leq L$, and this restriction also applies to Eqs. 20; therefore the maximization of E over ρ must be done with $0 \leq \rho \leq L$ and if the stationary point (Eq. 20) requires that $\rho > L$, then E is maximized with $\rho = L$. This results in the parametric equations

$$E(N_b) = \frac{LS}{2(1+L)\,N_b} - \frac{1}{2}\sum_{n_o} \ln\left(1 + L - L\frac{N_n}{N_b}\right) + \frac{L}{2}\sum_{n_o} \ln\frac{N_b}{N_n} - LR \tag{21a}$$

$$S(N_b) = \sum_{n_o} \frac{(1+L)^2\,(N_b - N_n)}{1 + L - L\frac{N_n}{N_b}}. \tag{21b}$$

Now consider what happens as $N \to \infty$. If we order the N_n so that $N_i < N_{i+1}$ we shall either reach a point where further increase in N just adds channels with $Q_n = 0$, or not. If we do, there are no problems in calculating S, E, and R, since additional Q_n will contribute nothing.

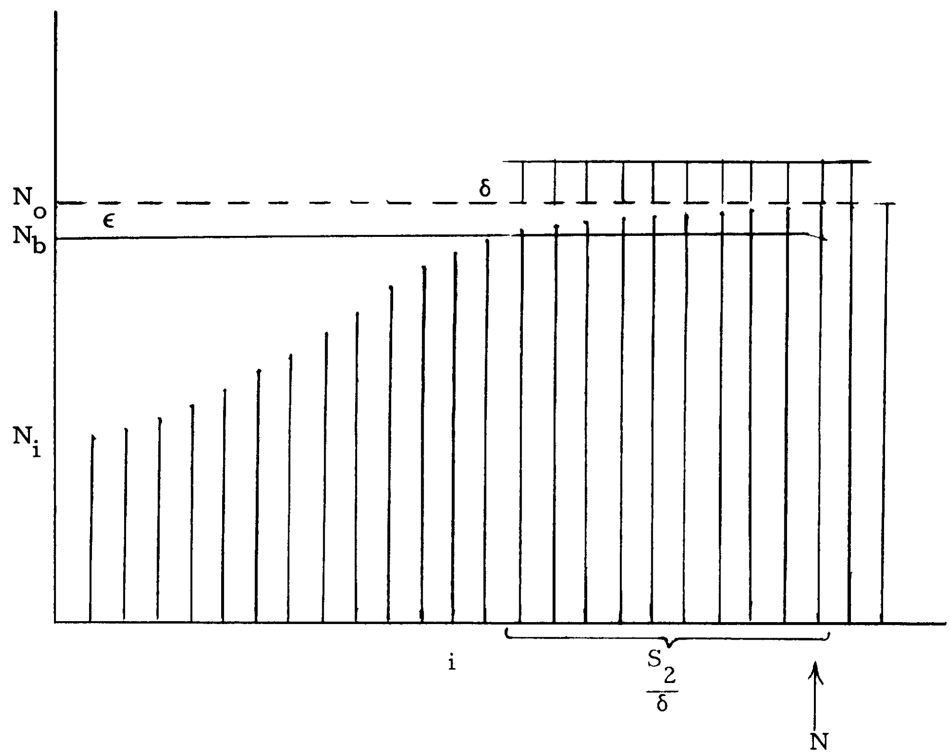


Fig. 4. Figure for limiting argument.

If we never reach such a point, we can use a limiting argument to get the solution. We use up some of the energy by setting $N_b = N_o - \epsilon$. As $\epsilon \to 0$, S, E, and R converge to S_1, E_1, and R_1 for any ρ (see Fig. 4). An additional amount of energy S_2 is uniformly distributed over S_2/δ additional channels, where $N_o \geq N_n > N_b$, with N_o a limit point of N_n. Each of these channels receives a signal energy δ. If we upper-bound the noise in these channels by N_o, we will only increase P_e and thus still have a bound. We can write for these channels

$$S_2 = \frac{S_2(1+\rho)(N_b' - N_o)}{\delta\left(1 + \rho - \rho \frac{N_o}{N_b'}\right)} \tag{22}$$

$$R_2 = \frac{S_2}{2\delta} \ln \frac{N_b'}{N_o}$$

$$E_2 = \frac{\rho S_2}{2(1+\rho)\, N_b'} - \frac{S_2}{2\delta} \ln \left(1 + \rho - \rho \frac{N_o}{N_b'}\right).$$

Equation 22 gives a limiting value of

$$N_b' \xrightarrow[\delta \to 0]{} \frac{\delta}{(1+\rho)} + N_o;$$

thus the other equations give

$$R \xrightarrow[\delta \to 0]{} \frac{S_2}{2(1+\rho)\, N_o}$$

$$E \xrightarrow[\delta \to 0]{} 0.$$

We let ϵ and δ both approach zero, thereby making $N \to \infty$, with the following results:

$$S = S_1 + S_2, \qquad S_2 = S - S_1$$

$$R = R_1 + R_2 = R_1 + \frac{S_2}{2(1+\rho)\, N_o} = R_1 + \frac{S - S_1}{2(1+\rho)\, N_o}$$

$$E = E_1 + E_2 = E_1.$$

2.2 EXPURGATED BOUND

At low rates, Elias,[4] Shannon,[20] and Gallager[8] have used various expurgation techniques to lower the random-coding upper bound on the achievable probability of error. We shall use a variation of Gallager's bound here because it is the tightest one and is applicable to a Gaussian channel.

Gallager's bound is generalized in Appendix C to a decoded list of L signals.

$$P_e \leq e^{-[E_o(\rho) - \rho R]}, \tag{23}$$

for any $\rho \geq L$, where

$$R = \ln 4eM - \frac{L}{\rho} \ln L,$$

$$E_o(\rho) = -\frac{\rho}{L} \ln \int_{\underline{x}_m} \cdots \int_{\underline{x}_{m_L}} P(\underline{x}_m) \cdots P\left(\underline{x}_{m_L}\right)$$

$$\left(\int_{\underline{y}} \left[P(\underline{y}/\underline{x}_m) \cdots P\left(\underline{y}/\underline{x}_{m_L}\right) \right]^{\frac{1}{L+1}} d\underline{y} \right)^{L/\rho} d\underline{x}_m \cdots d\underline{x}_{m_L} \tag{24}$$

for any $\rho \geq L$.

In order to apply this to a colored Gaussian channel, we use the same bounding techniques as before; the density $P(\underline{x})$, which is the same for all $P(\underline{x}_m)$, $P\left(\underline{x}_{m_i}\right)$, is constrained to a shell and bounded by a Gaussian function as in Eqs. 6 and 8. We write

$$P(\underline{x}_i) \leq \frac{e^{-rS+\delta r}}{q} \prod_{n=1}^{N} \frac{\exp\left(-\frac{x_{i,n}^2}{2Q_n} + x_{i,n}^2 r\right)}{\sqrt{2\pi Q_n}}.$$

We can replace S by $\Sigma\, Q_n$ and bring the rQ_n inside the product.

$P(\underline{y}/\underline{x}_i)$ is a multidimensional Gaussian density as in (5). To simplify notation, denote $\underline{x}_m$ by $\underline{x}_o$ and $\underline{x}_{m_i}$ by $\underline{x}_i$. Then from (24)

$$P_e \leq \left(\frac{e^\delta}{q}\right)^{\frac{L+1}{L}\rho} \exp[-E_e(\rho)+\rho R]$$

where now

$$E_e(\rho) = -\frac{\rho}{L} \sum_{n=1}^{N} \ln \int_{x_{0,n}} \cdots \int_{x_{L,n}} \frac{\exp\left(\sum_{i=0}^{L} \frac{-x_{i,n}^2}{2Q_n} + x_{i,n}^2 r - rQ_n \right)}{\left(\sqrt{2\pi Q_n}\right)^{L+1}}$$

$$\left[\int_{y_n} \frac{\exp - \sum_{i=0}^{L} \frac{(y_n - x_{i,n})^2}{2N_n(L+1)}}{\sqrt{2\pi N_n}} dy_n \right]^{L/\rho} dx_{0,n} \cdots dx_{L,n}. \tag{25}$$

The integral over y_n in Eq. 25 is

$$\int_{y_n} \prod_{i=0}^{L} \frac{e^{-\frac{(y_n - x_{i,n})^2}{2N_n(1+L)}}}{(\sqrt{2\pi N_n})^{\frac{1}{L+1}}} dy_n =$$

$$\int_{y_n} \frac{\exp\left(-\frac{y_n^2}{2N_n} + \frac{y_n}{(L+1)N_n}\sum_{i=0}^{L} x_{i,n} - \frac{1}{2(L+1)N_n}\sum_{i=0}^{L} x_{i,n}^2\right)}{\sqrt{2\pi N_n}} dy_n$$

$$= \exp\left[\frac{\left(\sum_{i=0}^{L} x_{i,n}\right)^2}{2N_n(L+1)^2} - \frac{\sum_{i=0}^{L} x_{i,n}^2}{2N_n(L+1)}\right] \int_{y_n} \frac{\exp\left\{-\frac{\left(y_n - \frac{1}{L+1}\sum_{i=0}^{L} x_{i,n}\right)^2}{2N_n}\right\}}{\sqrt{2\pi N_n}} dy_n.$$

Therefore the larger integral over all $x_{i,n}$,

$$\int_{x_{0,n}} \cdots \int_{x_{L,n}}$$

$$\frac{\exp\left\{\frac{-\sum_{i=0}^{L} x_{i,n}^2}{2Q_n} + \sum_{i=0}^{L} x_{i,n}^2 r_n - (1+L)r_n Q_n + \frac{L\left(\sum_{i=0}^{L} x_{i,n}\right)^2}{\rho 2N_n(L+1)^2} - \frac{L\sum_{i=0}^{L} x_{i,n}^2}{\rho N_n 2(L+1)}\right\}}{(2\pi Q_n)^{\frac{L+1}{2}}} dx_n,$$

can be converted into the form of a multivariate Gaussian density:

$$\int_{x_{0,n}} \cdots \int_{x_{L,n}} \exp\left(-\frac{1}{2|\xi|}\sum_{i=0}^{L}\sum_{j=0}^{L} |\xi|_{i,j} x_{i,n} x_{j,n}\right) dx_{0,n} \cdots dx_{L,n} \frac{\exp[-(L+1)r_n Q_n]}{(2\pi Q_n)^{\frac{L+1}{2}}},$$

where $|\xi|$ is the determinant of the correlation matrix, and $|\xi|_{i,j}$ is the cofactor of the i,j entry. We have

$$\frac{|\xi|_{i,j}}{|\xi|} = \begin{cases} -\frac{L}{\rho N_n(L+1)^2}; & \text{for } i \neq j \\ \frac{1}{Q_n} - 2r_n - \frac{L}{\rho N_n(L+1)^2} + \frac{L}{\rho N_n(L+1)} = \frac{1}{Q_n} - 2r_n + \frac{L^2}{\rho N_n(L+1)^2}; & i = j. \end{cases}$$

The integral is just

$$(2\pi)^{\frac{1+L}{2}} |\xi|^{1/2} \frac{e^{-(1+L)r_n Q_n}}{(2\pi Q_n)^{\frac{1+L}{2}}};$$

consequently, we need calculate only $|\xi|^{1/2}$. The expression $\frac{|\xi|_{i,j}}{|\xi|}$ is just the element of the inverse matrix and, since the determinant of the inverse matrix is the inverse of the determinant, the solution is easy. A matrix of order $1 + L$ with "a" on the diagonal and "b" off, has determinant $(a-b)^L(a+Lb)$. Thus

$$|\xi| = \frac{1}{\left[\frac{1}{Q_n} - 2r_n + \frac{L}{\rho N_n(1+L)}\right]^L \left[\frac{1}{Q_n} - 2r_n\right]}.$$

The integral becomes

$$\frac{e^{-(1+L)r_n Q_n}}{\left[1 - 2r_n Q_n + \frac{LQ_n}{\rho N_n(1+L)}\right]^{L/2} [1-2r_n Q_n]^{1/2}}.$$

Thus

$$E_o(\rho) = \frac{\rho(L+1)}{L} \sum_n r_n Q_n + \frac{\rho}{2} \sum_n \ln\left(1 - 2r_n Q_n + \frac{LQ_n}{\rho N_n(L+1)}\right) + \frac{\rho}{2L} \sum_n \ln(1-2r_n Q_n).$$

Making the substitution $\beta_n = r_n Q_n$, we have

$$E = E_o(\rho) - \rho R = \frac{\rho(L+1)}{L} \sum_n \beta_n + \frac{\rho}{2} \sum_n \ln\left(1 - 2\beta_n + \frac{LQ_n}{\rho N_n(L+1)}\right) + \frac{\rho}{2L} \sum_n \ln(1-2\beta_n) - \rho R, \tag{26}$$

which must be maximized, subject to the constraints

$$\beta_n \geq 0, \quad Q_n \geq 0, \quad \sum_{n=1}^{N} Q_n = S.$$

This maximization is done just as before, and gives the solution

$$Q_n = \begin{cases} \dfrac{\rho(1+L)^2 (N_b - N_n)}{L\left(1 + L - L\dfrac{N_n}{N_b}\right)}; & \text{for } N_n \leqslant N_b \\ 0; & \text{otherwise} \end{cases} \tag{27a}$$

$$\beta_n = \begin{cases} \dfrac{L\left(1 - \dfrac{N_n}{N_b}\right)}{2\left(1 + L - L\dfrac{N_n}{N_b}\right)}; & \text{for } N_n \leqslant N_b \\ 0; & \text{otherwise} \end{cases} \tag{27b}$$

$$r_n = \frac{L^2}{2\rho(1+L)^2 N_b}. \tag{27c}$$

Since

$$\sum_n \beta_n = \sum_n r_n Q_n = \frac{L^2}{2\rho(1+L)^2 N_b} \sum_n Q_n = \frac{L^2 S}{2\rho N_b (1+L)^2},$$

we can substitute the solutions of (27) in (26) and write

$$E = \frac{LS}{2N_b(1+L)} + \frac{\rho}{2} \sum_{n_o} \ln \frac{N_b}{N_n} - \frac{\rho}{2L} \sum_{n_o} \ln\left(1 + L - L\frac{N_n}{N_b}\right) - \rho R. \tag{28}$$

Equation 28 must now be maximized over ρ, where Eq. 27a gives the relation between ρ and N_b:

$$S = \sum_{n_o} \frac{\rho(1+L)^2 (N_b - N_n)}{L\left(1 + L - L\dfrac{N_n}{N_b}\right)}. \tag{29}$$

Consequently, we can write

$$\frac{dE}{d\rho} = \frac{\partial E}{\partial \rho} + \frac{\partial E}{\partial N_b} \frac{dN_b}{d\rho},$$

where $dN_b/d\rho$ is calculated from (29).

$$\frac{\partial E}{\partial \rho} = \frac{1}{2} \sum_{n_o} \ln \frac{N_b}{N_n} - \frac{1}{2L} \sum_{n_o} \ln\left(1 + L - L\frac{N_n}{N_b}\right) - R$$

$$\frac{\partial E}{\partial N_b} = -\frac{LS}{2(L+1)\, N_b^2} - \frac{\rho}{2}\sum_{n_o} \frac{\frac{N_n}{N_b^2}}{1 + L - L\frac{N_n}{N_b}} + \frac{\rho}{2}\sum_{n_o} \frac{1}{N_b} = 0.$$

The latter equality comes by substitution of the right side of Eq. 29 for S. Therefore

$$\frac{dE}{d\rho} = \frac{\partial E}{\partial \rho}.$$

Setting the derivative equal to zero, we have a stationary point at

$$\begin{aligned} R &= \frac{1}{2}\sum_{n_o} \ln\frac{N_b}{N_n} - \frac{1}{2L}\sum_{n_o} \ln\left(1 + L - L\frac{N_n}{N_b}\right) \\ E &= \frac{LS}{2N_b(1+L)}. \end{aligned} \tag{30}$$

Again, the expression for R is independent of ρ and depends only on N_b.

To show that the stationary point of (30) is a maximum, we use the same procedure as before; $dE/d\rho$ is monotone in N_b.

$$\frac{d}{dN_b}\left[\frac{dE}{d\rho}\right] = \frac{1}{2N_b}\sum_{n_o} \frac{(1+L)\left(1 - \frac{N_n}{N_b}\right)}{1 + L - L\frac{N_n}{N_b}} > 0,$$

and $dN_b/d\rho$ calculated from (29) is

$$\frac{dN_b}{d\rho} = -\frac{\sum_{n_o} \frac{N_b - N_n}{1 + L - L\frac{N_n}{N_b}}}{\sum_{n_o} \frac{\rho}{1 + L - L\frac{N_n}{N_b}}} < 0,$$

which proves that the stationary point is a maximum.

Because of the restriction that $\rho \geq L$ in Eq. 24, the same restriction applies in Eqs. 29 and 30. This complements Eqs. 20 and 21 to fill out the entire range of ρ.

Detailed calculations show that the slope of the E(R) function for fixed S is $-\rho$ for all three equations (20), (21), and (30). It can be seen from the form of the equations (3) and (23) that if a slope or dE/dR exists it must be $-\rho$, since one can operate anywhere

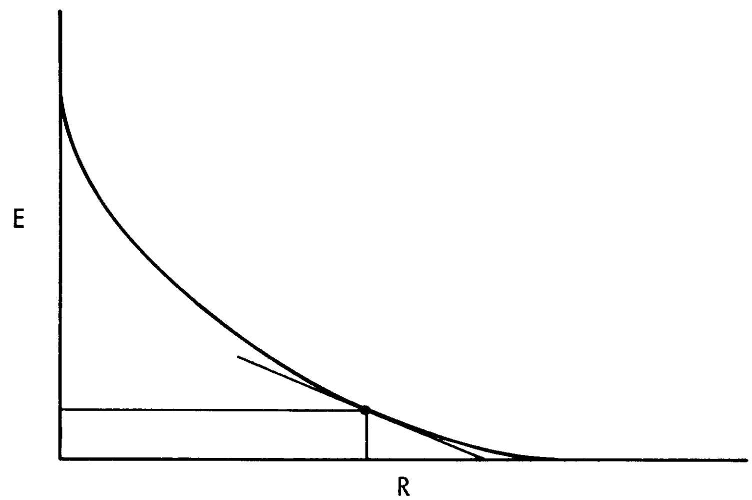


Fig. 5. Figure for derivative argument.

along the straight line of slope $-\rho$ shown in Fig. 5. The optimum E(R) must lie above this straight line in order to be an optimum and thus can only have slope $-\rho$ at $R(\rho)$ and $E(\rho)$.

2.3 ASYMPTOTIC EXPRESSION FOR E, R, AND S

In the bounds obtained here we have found parametric expressions for three quantities R, S, and E, for any finite T. Because the three expressions are dependent on the set N_n they will change as T is increased. Fortunately, as $T \to \infty$ these three expressions approach an asymptotic form. If we are to have an average power constraint, it would be desirable if, for fixed ρ and N_b,

$$\lim_{T\to\infty} \frac{S}{T} = P,$$

and if we are to be able to transmit at some time rate R_t, it would be desirable if

$$\lim_{T\to\infty} \frac{R}{T} = R_t.$$

Such is the case, as indicated by the following theorem.

THEOREM: Given a noise autocorrelation function $\mathcal{R}(\tau)$ and its Fourier transform

$$N(w) = \int_{-\infty}^{\infty} \mathcal{R}(\tau)\, e^{-jw\tau}\, d\tau,$$

commonly called the noise power density spectrum, then the eigenvalue solutions (N_i) to the integral equation

$$\int_0^T \phi_i(\tau)\, \mathcal{R}(t-\tau)\, d\tau = N_i\phi_i(t), \qquad 0 \le t \le T$$

have the property

$$\lim_{T\to\infty} \frac{\sum_{i=1}^{\infty} G(N_i)}{T} = \frac{1}{2\pi}\int_{-\infty}^{\infty} G[N(w)]\, dw,$$

if the integral exists, where $G(\cdot)$ is monotone nonincreasing and bounded.

This theorem is proved in the appendix.

We observe that in the expression for R (Eq. 20b)

$$G(x) = \begin{cases} \ln \dfrac{N_b}{x}; & \text{for } x \le N_b \\ 0; & \text{otherwise,} \end{cases}$$

which is monotone nonincreasing and bounded as long as x stays away from zero; consequently,

$$\lim_{T\to\infty} \frac{R}{T} = \frac{1}{4\pi} \int_{N(w)\le N_b} \ln \frac{N_b}{N(w)}\, dw = R_t,$$

as long as N(w) is bounded away from 0. Also, in the expression for S (Eq. 20c)

$$G(x) = \begin{cases} \dfrac{(1+\rho)^2 (N_b-x)}{1+\rho-\rho\dfrac{x}{N_b}}; & x \le N_b \\ 0; & \text{otherwise} \end{cases}$$

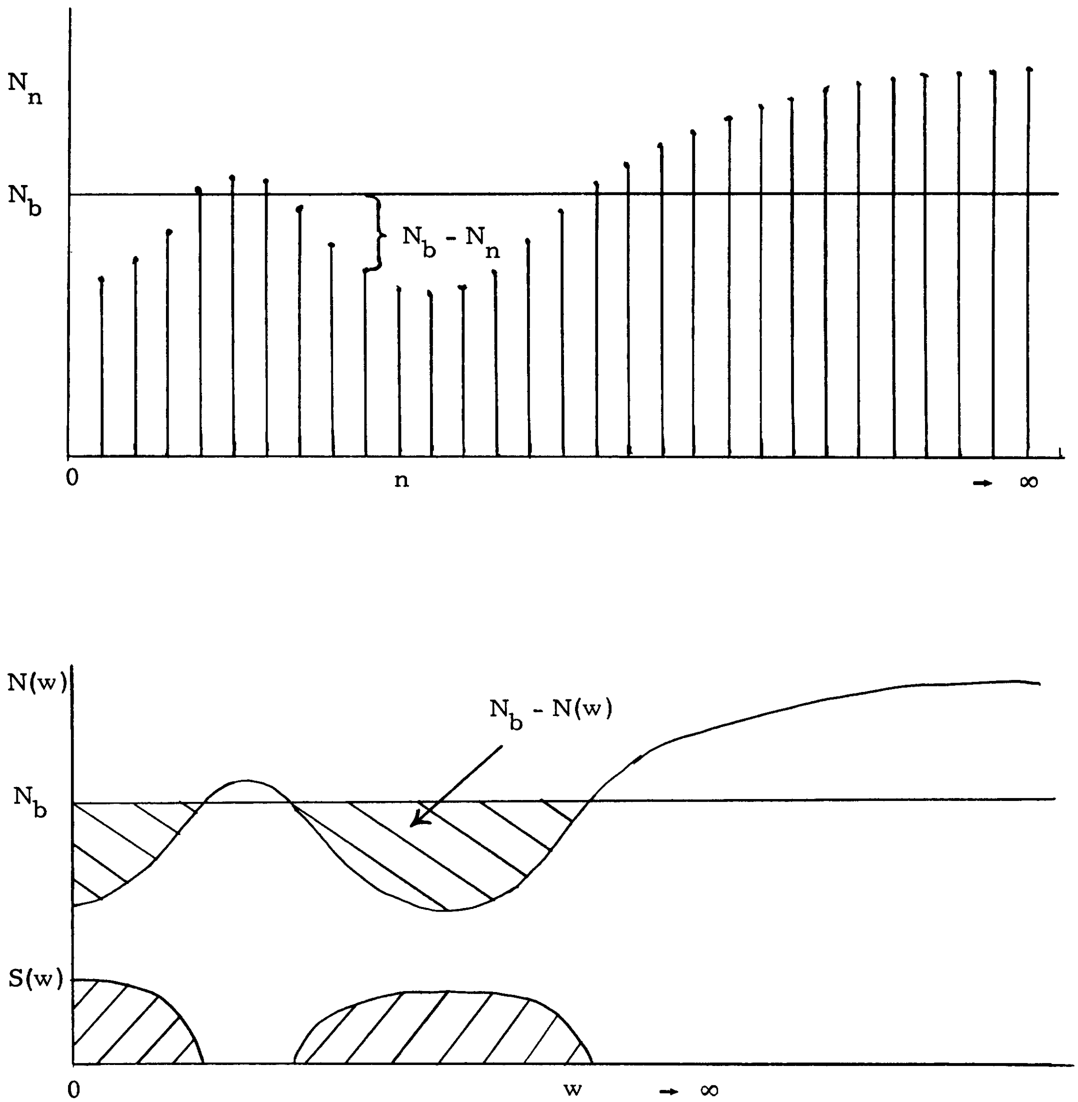
which is monotone nonincreasing and bounded; consequently,

$$\lim_{T\to\infty} \frac{S}{T} = \frac{1}{2\pi} \int_{N(w)\le N_b} \frac{(1+\rho)(N_b-N(w))}{1+\rho-\rho\dfrac{N(w)}{N_b}}\, dw = P.$$

We have already defined the exponent as $\lim_{T\to\infty} \frac{E}{T}$. The part of E which contains a sum over the eigenfunction channels has

$$G(x) = \begin{cases} \ln\left(1+\rho-\rho\dfrac{x}{N_b}\right); & x \le N_b \\ 0; & \text{otherwise} \end{cases}$$

Consequently, we have



Note; $S(w) = N_b - N(w)$ only when $\rho = 0$

Fig. 6. Solutions to the signal power-distribution problem.

$$\lim_{T\to\infty} \frac{E}{T} = \frac{P}{2(1+\rho)\, N_b} - \frac{1}{4\pi} \int_{N(w)\leq N_b} \left(\ln\, 1 + \rho - \rho \frac{N(w)}{N_b}\right) dw.$$

The expressions for the expurgated bound can be treated in exactly the same way, to obtain

$$\lim_{T\to\infty} \frac{R}{T} = \frac{1}{4\pi} \int_{N(w)\leq N_b} \left\{ \ln \frac{N_b}{N(w)} - \frac{1}{L} \ln \left(1 + L - L \frac{N(w)}{N_b}\right)\right\} dw,$$

$$\lim_{T\to\infty} \frac{S}{T} = \frac{1}{2\pi} \int_{N(w)\leq N_b} \frac{\rho(1+L)^2\, (N_b - N(w))}{L\left(1 + L - L\frac{N(w)}{N_b}\right)} dw = P,$$

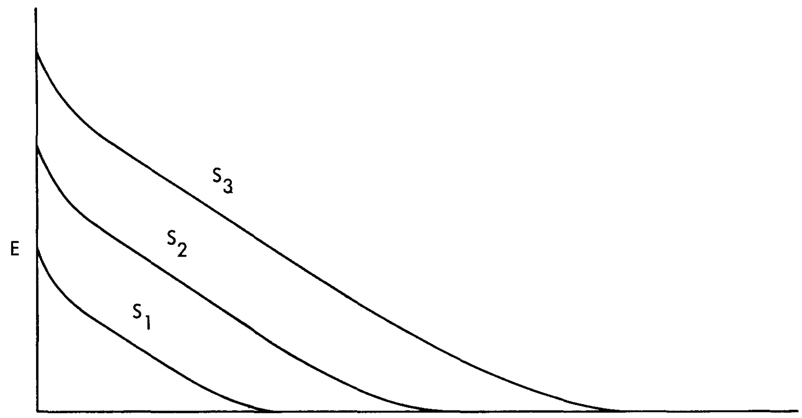
$$\lim_{T\to\infty} \frac{E}{T} = \frac{LP}{2N_b(1+L)}.$$

A typical solution is shown in Fig. 6.

2.4 GRAPHIC PRESENTATION OF UPPER BOUND

Thus far we have derived expressions for the functions E, R, and S in terms of the parameters ρ and N_b. By varying ρ and N_b and using the appropriate equations (20), (21), or (29) and (30), we are able to cover the entire ranges of S and R. Usually a family of E(R) functions is presented, each curve having a different value of S. A typical example is shown in Fig. 7a. As an alternative we can hold R constant and find E as a function of S as is shown in Fig. 7b. The latter representation is somewhat more natural for the parametric equation solution that we have found because over most of the range a constant R implies a constant N_b, with the result that E and S are parametric functions of ρ. While in the E(R) presentation we had $\frac{dE}{dR} = -\rho$ everywhere, in the E(S) presentation dE/dS takes on the three different values.

$$\frac{dE}{dS} = \begin{cases} \dfrac{\rho}{2(1+\rho)\, N_b}, & \text{for } \rho \leq L \quad \text{(here } N_b \text{ is fixed)} \\[2ex] \dfrac{L}{2(1+L)\, N_b}, & \text{for } \rho = L \quad \text{(here } N_b \text{ increases)} \\[2ex] \dfrac{L}{2(1+L)\, N_b}, & \text{for } \rho > L \quad \text{(here } N_b \text{ is fixed)} \end{cases}$$



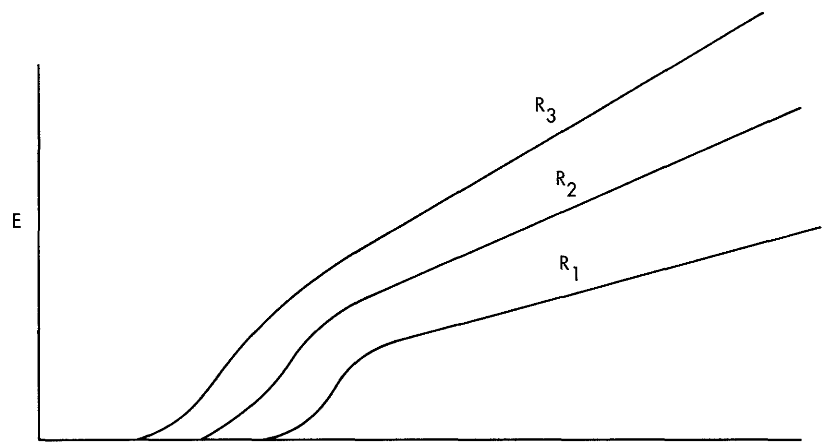


Fig. 7. Graphic presentation of results.

The derivative for $\rho > L$ is just a constant since E is a linear function of S there.

2.5 COMMENTS ON SIGNAL DESIGN

We have derived an upper bound on the achievable probability of error under the assumption that the signals were to be detected by a maximum-likelihood receiver, which is the receiver with the lowest probability of error for equally likely signals. Usually maximum-likelihood receivers are hard to build and one has to be satisfied with a somewhat poorer but simpler receiver, and it could be true that the simpler receiver would require an entirely different set of signals to minimize the probability of error. The situation is not hopeless though, since the simple receiver is trying to emulate a maximum-likelihood receiver and one would expect that the closer it comes to this goal the more it would require signals like those used here. However, some recent work done by G. D. Forney[7] shows that block length is not necessarily the all-important parameter in receiver complexity; that one might obtain better performance by increasing the block length and using an inferior receiver than by using fixed block length and trying harder to emulate a maximum-likelihood receiver.

Leaving aside these considerations, the signals that we used were chosen at random from a multidimensional Gaussian ensemble constrained to be on a shell. This ensemble is obviously not Gaussian nor independent, but as $T \to \infty$ the individual density of each component of the signal approaches Gaussian with energy Q_n. The signals can be generated sequentially with each coordinate distributed conditionally on those coordinates already generated. The distribution will not be overly complicated because it depends only on the sum of the previous coordinates squared and the noise power in the coordinate that is being generated. It may be possible to use one of Wozencraft's[24] convolutional coders to choose the coordinate value subject to the conditioning probability.

The signals needed for the expurgated bound are not so clearly defined. Besides requiring the signals to have a certain energy we have expurgated the "bad" half of the signals. Which signals are bad is not easily detected, since the determination of "bad" signal is only made in context with the other $M - 1$ signals.

III. LOWER BOUND TO THE AVERAGE PROBABILITY OF ERROR

3.1 SPHERE-PACKING BOUND

We shall consider the same model that we considered in Section I but now we are interested in a lower bound to the average probability of error. We shall calculate a a P_e that cannot be reduced by any coder-decoder system operating over the constraint time T. This bound is called, for historical reasons, the "sphere-packing bound." The original derivation was done by packing the received signal space with spheres, one around each transmitted signal. We now use a theorem of Gallager[21] which states:

Let a code consist of M equiprobable code words $(\underline{x}_1 \dots \underline{x}_M)$. Define $f(\underline{y})$ as an arbitrary probability measure on the output space and define $\mu_m(s)$ for each m as

$$\mu_m(s) = \ln \int_{\text{all } \underline{y}} f(\underline{y})^s \, P(\underline{y}/\underline{x}_m)^{1-s} \, d\underline{y}, \qquad s \geq 0. \tag{31}$$

Let

$$Z_m = \int_{Y_m} f(\underline{y}) \, dy,$$

where Y_m is that set of $\underline{y}$ for which m is on the list. Then if $s \geq 0$ is chosen to satisfy

$$Z_m \leq \frac{1}{4} \exp\left[\mu_m(s) + (1-s)\mu_m'(s) - (1-s)\sqrt{2\mu_m''(s)}\right], \tag{32}$$

the probability of error, given input m, is lower-bounded by

$$P_{em} \geq \frac{1}{4} \exp\left[\mu_m(s) - s\mu_m'(s) - s\sqrt{2\mu_m''(s)}\right]. \tag{33}$$

The proof of this theorem is given in Appendix D.

We then use this theorem to bound the average probability of error by finding a lower bound to the P_e for the worst code word and from this finding a bound on the average, P_e.

First, we shall restrict ourselves to signals with small energy, since they are the best candidates for being poor signals. If the average energy of all possible signals is S or less,

$$\frac{1}{M} \sum_{n=1}^{N} \sum_{m=1}^{M} x_{nm}^2 \leq S = TP,$$

where x_{nm} is the value of the n^{th} coordinate of the m^{th} signal. Then at least αM of the signals will have energy

$$\sum_{n=1} x_{nm}^2 \leq \frac{S}{1-\alpha}, \qquad 0 < \alpha < 1.$$

We must also restrict the range of two other sums in order to obtain a bound on P_e. The sums are

$$\sum_{n_o} x_{nm}^2, \tag{34}$$

and

$$\sum_{n_o} x_{nm}^2 N_n. \tag{35}$$

The set n_o is defined as all n such that $N_n \leq N_b$, where N_b is analogous to the N_b of Section II and is given by the implicit relation

$$R = \frac{1}{2} \sum_{n_o} \ln \frac{N_b}{N_n} + \ln \frac{4S^2}{\alpha\epsilon^2(1-\alpha)^2} + 2\sqrt{\sum_{n_o} \frac{(N_b-N_n)^2}{N_b^2} + \frac{2S}{N_b(1-\alpha)}}. \tag{36}$$

While it is true that there is no solution for N_b for some R and S, one can be assured that if R and S grow linearly with T there will be a solution for sufficiently large T.

We now observe that the sums of (34) and (35) are bounded above by $\frac{S}{1-\alpha}$ and $N_b \frac{S}{1-\alpha}$, respectively, and below by zero. If we split up the ranges into sections ϵ by ϵN_b, we shall have at most $\frac{S^2}{\epsilon^2(1-\alpha)^2}$ sections, each ϵ by ϵN_b in size. One of these ϵ by ϵN_b sections will have at least

$$\frac{\alpha M \epsilon^2 (1-\alpha)^2}{S^2}$$

code words and we shall constrain our analysis to this subset of code words. Now,

$$K \leq \sum_{n_o} x_{nm}^2 \leq K + \epsilon \tag{37}$$

and

$$J \leq \sum_{n_o} x_{nm}^2 N_n \leq J + \epsilon N_b,$$

K and J being functions of the signal set.

Among these $\frac{\alpha M\epsilon^2(1-\alpha)^2}{S^2}$ signals there will be one signal (call it m), with

$$Z_m \leq \frac{LS^2}{\alpha M\epsilon^2(1-\alpha)^2}.$$

This follows from the fact that there are exactly L messages on the list for each $\underline{y}$, and therefore

$$\sum_{m=1}^{M} Z_m = \sum_{m=1}^{M} \int_{y_m} f(\underline{y})\, d\underline{y} = \int_y Lf(\underline{y})\, d\underline{y} = L.$$

For the m above, inequality (32) will be met if

$$\frac{S^2L}{\epsilon^2(1-\alpha)^2\,\alpha M} \leq \frac{1}{4}\exp\left[\mu_m(s) + (1-s)\mu_m'(s) - (1-s)\sqrt{2\mu_m''(s)}\right].$$

Taking the logarithm of both sides and recalling that $\frac{M}{L} = e^R$, we find this equivalent to

$$R \geq -\mu_m(s) - (1-s)\mu_m'(s) + (1-s)\sqrt{2\mu_m''(s)} + \ln\frac{4S^2}{\alpha\epsilon^2(1-\alpha)^2}. \tag{38}$$

We must therefore choose f(y) and s to meet Eq. 38. We know that

$$P(\underline{y}/\underline{x}_m) = \prod_n \frac{\exp\dfrac{-(y_n-x_{nm})^2}{2N_n}}{\sqrt{2\pi N_n}}.$$

Let us choose

$$f(\underline{y}) = \prod_n \frac{\exp\dfrac{-y_n^2}{2Q_n}}{\sqrt{2\pi Q_n}}.$$

By integration of (31), we have

$$\mu_m(s) = -\frac{1}{2}\sum_n \frac{x_{nm}^2 s(1-s)}{Q_n(1-s) + N_n s} - \frac{1}{2}\sum_n \ln\left[Q_n(1-s) + N_n s\right]$$

$$+\frac{1}{2}s\sum_n \ln N_n + \frac{1}{2}(1-s)\sum_n \ln Q_n.$$

Then

$$\mu'_m(s) = -\frac{1}{2}\sum_n \frac{N_n - Q_n}{(1-s)Q_n + N_n s}$$

$$-\frac{1}{2}x_{nm}^2 \sum_n \frac{[Q_n(1-s)+N_n s](1-2s) - s(1-s)(N_n-Q_n)}{[Q_n(1-s)+N_n s]^2}$$

$$+\frac{1}{2}\sum_n \ln N_n - \frac{1}{2}\sum_n \ln Q_n,$$

and

$$\mu''_m(s) = \frac{1}{2}\sum_n \frac{(N_n-Q_n)^2}{[Q_n(1-s)+N_n s]^2} + \sum_n x_{nm}^2 \frac{Q_n N_n}{[Q_n(1-s)+N_n s]^3}.$$

An appropriate choice of Q_n will simplify these equations significantly. Let

$$Q_n = \begin{cases} N_n; & \text{for } N_n > N_b; \quad \text{call this set } n_1 \\ \dfrac{N_b - sN_n}{1-s}; & \text{for } N_n \leq N_b; \quad \text{call this set } n_o, \end{cases}$$

where N_b is given by (36). Remember that the derivatives of $\mu_m(s)$ are taken with f(y) fixed and that Q_n being a function of s does not change these derivatives. The fact that this choice of Q_n both simplifies the expression and gives an exponentially tight bound is indeed fortuitous. The expression becomes

$$-\mu_m(s) - (1-s)\mu'_m(s) + (1-s)\sqrt{2\mu''_m(s)}$$

$$= \frac{(1-s)}{2N_b}\sum_{n_o} x_{nm}^2 - \frac{s(1-s)}{2N_b^2}\sum_{n_o} x_{nm}^2 N_n - \frac{1}{2}\sum_{n_o}\frac{N_b - N_n}{N_b}$$

$$+\frac{1}{2}\sum_{n_o}\ln\frac{N_b}{N_n} + \frac{(1-s)^2}{2}\sum_{n_1}\frac{x_{nm}^2}{N_n} + (1-s)\sqrt{2\mu''_m(s)}. \tag{39}$$

By substituting (39) in (38), Eq. 38 becomes

$$R \geq \frac{(1-s)}{2N_b} \sum_{n_o} x_{nm}^2 - \frac{s(1-s)}{2N_b^2} \sum_{n_o} x_{nm}^2 N_n - \frac{1}{2} \sum_{n_o} \frac{N_b - N_n}{N_b}$$

$$+ \frac{1}{2} \sum_{n_o} \ln \frac{N_b}{N_n} + \frac{(1-s)^2}{2} \sum_{n_1} \frac{x_{nm}^2}{N_n} + (1-s) \sqrt{2\mu_m''(s)} + \ln \frac{4S^2}{\alpha\epsilon^2(1-\alpha)^2}. \tag{40}$$

We observe that

$$\mu_m''(s) \leq \frac{1}{2} \sum_{n_o} \frac{(N_b - N_n)^2}{N_b^2 (1-s)^2} + \frac{S}{N_b (1-s)^2 (1-\alpha)}, \tag{41}$$

and

$$\sum_{n_1} \frac{x_{nm}^2}{N_n} \leq \frac{1}{N_b} \left[\sum_n x_{nm}^2 - \sum_{n_o} x_{nm}^2 \right] \leq \frac{S}{N_b(1-\alpha)} - \frac{1}{N_b} \sum_{n_o} x_{nm}^2. \tag{42}$$

We now use Eqs. 41, 36, 37, and 42 to show that (40) will be met if

$$0 \geq \frac{(1-s)^2 S}{2N_b(1-\alpha)} + \frac{s(1-s)}{2N_b} (K+\epsilon) - \frac{s(1-s)}{2N_b^2} J - \frac{1}{2} \sum_{n_o} \frac{N_b - N_n}{N_b}$$

$$- \sqrt{\sum_{n_o} \frac{(N_b - N_n)^2}{N_b^2} + \frac{2S}{N_b(1-\alpha)}}. \tag{43}$$

To review the logic thus far, we note that if (43) is met and N_b is chosen to meet (36), then Eq. 32 will be met and Eq. 33 will bound P_e.

We now claim that (43) will either be met with equality for some $0 \leq s \leq 1$ or will still be true for $s = 0$. We see that the right side of (43) must be negative at $s = 1$. Therefore, since the right side of (43) is continuous in s, it must pass through zero as s goes from 1 to 0 or still be negative at $s = 0$. In either case, for some s, we have

$$-\ln P_{em} \leqslant \ln 4 - \mu_m(s) + s\mu_m'(s) + s\sqrt{2\mu_m''(s)}$$

$$= \ln 4 + \frac{1}{2}\sum_{n_o} x_{nm}^2 \frac{s^2 N_n}{N_b^2} - \frac{1}{2}\sum_{n_o} \ln \frac{N_b - sN_n}{N_b(1-s)} + \frac{s}{2}\sum_{n_o} \frac{N_b - N_n}{N_b(1-s)}$$

$$+ \frac{s^2}{2}\sum_{n_1} \frac{x_{nm}^2}{N_n} + s\sqrt{2\mu_m''(s)}$$

$$\leqslant \ln 4 + \frac{s^2(J+\epsilon N_b)}{2N_b^2} - \frac{1}{2}\sum_{n_o} \ln \frac{N_b - sN_n}{N_b(1-s)} + \frac{s}{2}\sum_{n_o} \frac{N_b - N_n}{N_b(1-s)}$$

$$\frac{s^2}{2}\sum_{n_1} \frac{x_{nm}^2}{N_n} + \frac{s}{1-s}\sqrt{\sum_{n_o} \frac{(N_b - N_n)^2}{N_b^2} + \frac{2S}{N_b(1-\alpha)}}. \tag{44}$$

If inequality (43) is met at $s = 0$, then

$$-\ln P_e \leqslant \ln 4.$$

Otherwise, (43) is met with equality for some s, and by using it to express J in terms of the other parameters and by using (42), Eq. 44 becomes

$$-\ln P_{em} \leqslant \ln 4 + \frac{2S}{2N_b(1-\alpha)} - \frac{1}{2}\sum_{n_o} \ln \frac{N_b - sN_n}{N_b(1-s)} + \frac{s^2\epsilon}{N_b}. \tag{45}$$

Inequality (45) is met for some s between 1 and 0, but if we find the s that maximizes the right side of (45), we can be sure that that is a bound on P_e. Setting the derivative of the right side of (45) with respect to s equal to zero, we have

$$\frac{S}{2N_b(1-\alpha)} - \frac{1}{2}\sum_{n_o} \frac{(1-s)(-N_n) + N_b - sN_n}{(1-s)(N_b - sN_n)} + \frac{2s\epsilon}{N_b} = 0$$

or

$$S = (1-\alpha)\sum_{n_o} \frac{N_b(N_b - N_n)}{(1-s)(N_b - sN_n)} - 4(1-\alpha)\, s\epsilon. \tag{46}$$

This is a maximum, as the second derivative is

$$-\frac{1}{2}\sum_{n_o} \frac{(N_b - N_n)(N_b - sN_n + N_n(1-s))}{(N_b - sN_n)^2 (1-s)^2} + \frac{2\epsilon}{N_b} < 0 \quad \text{for } \epsilon \text{ small enough.}$$

We have obtained a bound on P_{em} for one code word in any code. Therefore if we double the number of code words, then all of the added code words must have a P_e equal or larger than P_{em} (otherwise we could have used one of the added code words instead of m and done better). For the larger code,

$$E = -\ln \overline{P}_e \leq \frac{sS}{2N_b(1-\alpha)} - \frac{1}{2}\sum_{n_o} \ln\frac{N_b - sN_n}{N_b(1-s)} + \ln 8 + \frac{s^2\epsilon}{N_b}$$

$$R = \frac{1}{2}\sum_{n_o} \ln\frac{N_b}{N_n} + \ln\frac{8S^2}{\alpha\epsilon^2(1-\alpha)^2} + 2\sqrt{\sum_{n_o}\frac{(N_b-N_n)^2}{N_b^2} + \frac{2S}{N_b(1-\alpha)}}, \tag{47}$$

where S is determined by

$$S = (1-\alpha)\sum_{n_o}\frac{N_b(N_b-N_n)}{(1-s)(N_b-sN_n)} - 4(1-\alpha)\, s\epsilon.$$

Now we show that if s takes on any other value than that determined by (46), a contradiction will result. We choose $\alpha = 1/T$, substitute $\rho'/(1+\rho')$ for s, and evaluate

$$\lim_{T\to\infty}\frac{S}{T} = \frac{1}{T}\sum_{n_o}\frac{(1+\rho')^2\,(N_b-N_n)}{1+\rho'-\rho'\dfrac{N_n}{N_b}} = P$$

$$\lim_{T\to\infty}\frac{E}{T} = \frac{\rho' P}{2(1+\rho')N_b} - \frac{1}{2T}\sum_{n_o}\ln\left(1+\rho'-\rho'\frac{N_n}{N_b}\right)$$

$$\lim_{T\to\infty}\frac{R}{T} = \frac{1}{2T}\sum_{n_o}\ln\frac{N_b}{N_n}.$$

The radical expression in R disappears because it only grows with $\sqrt{T}$. These are exactly the same expressions that we obtained as an upper bound on P_e in Section II. There we had maximized E over ρ and found a single maximum point. Therefore if the lower bound E is to be equal to or larger than the upper bound E, as it must be, ρ' must equal ρ. This means that the bound obtained by maximizing (45) over s is exponentially as tight as possible.

The argument above also shows that the exponents of the upper and lower bounds are the same for $\rho \leq L$. Thus the random-coding bound derived in Section II is also exponentially tight for $\rho \leq L$, and gives the true value of E(R). If we restrict ourselves to the bound given by Eqs. 32 and 33 (the sphere-packing bound), we cannot hope to get an exponentially tighter bound than we have for any $\rho \neq \infty$, even when the list size is 1. The only way that L appears in the bound is as an ln L term in the rate. Consequently the optimization of the bound does not depend on L at all, as long as L is independent of T, and if we have optimized it for large $L < \infty$, we have optimized it for $L = 1$.

3.2 SPHERE-PACKING BOUND FOR KNOWN SIGNAL POWER

We shall derive a bound on P_e when the average power in each channel is fixed. In other words, the code is constrained to have

$$\frac{1}{M} \sum_{m=1}^{M} x_{nm}^2 = S_n,$$

where S_n is the average energy in the n^{th} channel, and x_{nm} is the n^{th} component of the m^{th} code word. This bound can be used to determine a lower bound on P_e when the power density spectrum of the transmitter is known.

We now have

$$\sum_n S_n = S.$$

The bounding procedure is very similar to that used before, and in order to maintain a resemblance to the proof in 3.1, we shall use an artifice. In section 3.1 we obtained a parameter N_b which was instrumental in determining the quantities S, R, and E. Here we define a parameter N_{bn} which is variable over n but eventually takes the place of N_b in the formulations

$$S_n = \frac{N_{bn}(N_{bn}-N_n)}{(1-p)(N_{bn}-pN_n)} \tag{48}$$

The defining equation (48) has two values of N_{bn}, but we are only interested in $N_{bn} \geq N_n$ and this N_{bn} is unique for any $S_n \geq 0$. We now define

$$Q_n = \frac{N_{bn} - sN_n}{(1-s)},$$

and proceed as in section 3.1. With this modified definition of Q_n, we have

$$-\mu_m(s) - (1-s)\mu_m'(s) + (1-s)\sqrt{2\mu_m''(s)}$$

$$= \frac{1-s}{2} \sum_n \frac{x_{nm}^2}{N_{bn}} - \frac{s(1-s)}{2} \sum_n \frac{x_{nm}^2 N_n}{N_{bn}^2} - \frac{1}{2} \sum_n \frac{N_{bn} - N_n}{N_{bn}}$$

$$+ \frac{1}{2} \sum_n \ln \frac{N_{bn}}{N_n} + (1-s)\sqrt{2\mu_m''(s)}.$$

The term in this analysis that is instrumental in bounding E is the sum:

$$\sum_n \frac{x_{nm}^2}{N_{bn}} = \sum_n \frac{x_{nm}^2(N_{bn}-N_n)}{S_n(1-p)(N_{bn}pN_n)}.$$

We observe that

$$\overline{\sum_n \frac{x_{nm}^2}{N_{bn}}}^{(m)} = \sum_n \overline{\frac{x_{nm}^2}{N_{bn}}}^{(m)} = \sum_n \frac{N_{bn} - N_n}{(1-p)(N_{bn}-pN_n)},$$

and at least αM of the signals have

$$\sum_n \frac{x_{nm}^2}{N_{bn}} \leqslant \sum_n \frac{N_{bn} - N_n}{(1-\alpha)(1-p)(N_{bn}-pN_n)} = \sum_n \frac{S_n}{(1-\alpha)N_{bn}}. \tag{49}$$

Now there is only one sum that must be constrained to an ϵ interval,

$$\sum_n \frac{x_{nm}^2 N_n}{N_{bn}^2},$$

which is bounded above by

$$\sum_n \frac{x_{nm}^2 N_n}{N_{bn}^2} \leqslant \sum_n \frac{x_{nm}^2}{N_{bn}} \leqslant \frac{1}{1-\alpha} \sum_n \frac{S_n}{N_{bn}}.$$

Consequently, there will be some ϵ interval with at least $\dfrac{\alpha M\epsilon(1-\alpha)}{\sum_n \frac{S_n}{N_{bn}}}$ signals. We shall consider only this subset of signals for which

$$J \leqslant \sum_n \frac{x_{nm}^2 N_n}{N_{bn}^2} \leqslant J + \epsilon. \tag{50}$$

Gallager's theorem may then be stated: If

$$R \geqslant \frac{1-s}{2} \sum_n \frac{x_{nm}^2}{N_{bn}} - \frac{s(1-s)}{2} \sum_n \frac{x_{nm}^2 N_n}{N_{bn}^2} - \frac{1}{2} \sum_n \frac{N_{bn} - N_n}{N_{bn}}$$

$$+ \frac{1}{2} \sum_n \ln \frac{N_{bn}}{N_n} + (1-s)\sqrt{2\mu_m''(s)} + \ln \frac{4 \sum_n \frac{S_n}{N_{bn}}}{\alpha\epsilon(1-\alpha)}, \tag{51}$$

then

$$E_m \leq \frac{s^2}{2}\sum_n \frac{x_{nm}^2 N_n}{N_{bn}^2} - \frac{1}{2}\sum_n \ln \frac{N_{bn}-sN_n}{N_{bn}(1-s)} + \frac{s}{2}\sum_n \frac{N_{bn}-N_n}{N_{bn}(1-s)} + s\sqrt{2\mu_m''(s)} + \ln 4. \tag{52}$$

Using (49) and (50) and the fact that

$$\mu''(s) \leq \frac{1}{2}\sum_n \frac{(N_{bn}-N_n)^2}{(1-s)^2 N_{bn}^2} + \sum_n \frac{S_n}{(1-\alpha)(1-s)^2 N_{bn}},$$

we claim that if

$$R \geq \frac{1-s}{2(1-\alpha)}\sum_n \frac{S_n}{N_{bn}} - \frac{s(1-s)}{2} J - \frac{1}{2}\sum_n \frac{N_{bn}-N_n}{N_{bn}} + \frac{1}{2}\sum_n \ln \frac{N_{bn}}{N_n}$$
$$+ (1-s)\sqrt{\sum_n \frac{(N_{bn}-N_n)^2}{(1-s)^2 N_{bn}^2} + \sum_n \frac{S_n}{(1-\alpha)(1-s)^2 N_{bn}}}$$
$$+ \ln \frac{4}{\alpha\epsilon(1-\alpha)}\sum_n \frac{S_n}{N_{bn}}, \tag{53}$$

then (51) will be met, and E_m will be bounded by (52). We now choose p so that

$$R = \frac{1}{2}\sum_n \ln \frac{N_{bn}}{N_n} + 2\sqrt{\sum_n \frac{(N_{bn}-N_n)^2}{N_{bn}^2} + \sum_n \frac{S_n}{(1-\alpha)N_{bn}}}$$
$$+ \frac{\epsilon}{2} + \frac{\alpha}{2(1-\alpha)}\sum_n \frac{S_n}{N_{bn}} + \ln \frac{4}{\alpha\epsilon(1-\alpha)}\sum_n \frac{S_n}{N_{bn}}. \tag{54}$$

This can be done as long as R grows linearly with T by making α sufficiently small and p sufficiently close to 1. As $p \to 1$, $N_{bn} \to N_n$.

When we substitute (54) in (53), we obtain

$$0 \geq \frac{(1-s)}{2(1-\alpha)}\sum_n \frac{S_n}{N_{bn}} - \frac{s(1-s)}{2} J - \frac{1}{2}\sum_n \frac{N_{bn}-N_n}{N_{bn}}$$
$$- \sqrt{\sum_n \frac{(N_{bn}-N_n)^2}{N_{bn}^2} + \sum_n \frac{S_n}{(1-\alpha)N_{bn}}} - \frac{\epsilon}{2} - \frac{\alpha}{2(1-\alpha)}\sum_n \frac{S_n}{N_{bn}}. \tag{55}$$

Equation 55 is clearly met when $s = 1$, and since the right side is continuous in s, we are again assured that either it will be met with equality for some $s \geq 0$ or it is still met with $s = 0$. Then solving (55) for J and substituting that solution in (52), we know that either

$$E_m \leq \left(\frac{s}{2} - \frac{s^2\alpha}{2(1-\alpha)(1-s)}\right) \sum_n \frac{S_n}{N_{bn}} - \frac{1}{2} \sum_n \ln \frac{N_{bn} - sN_n}{N_{bn}(1-s)}$$

$$+ \frac{s\epsilon}{2}\left(s - \frac{1}{1-s}\right) + \ln 4 + s\sqrt{2\mu_m''(s)}$$

$$- \frac{s}{1-s}\sqrt{\sum_n \frac{(N_{bn}-N_n)^2}{N_{bn}^2} + \sum_n \frac{S_n}{(1-\alpha)N_{bn}}},$$

for some $1 \geq s \geq 0$, or

$$E_m \leq \ln 4.$$

Bounding several of the terms and using the same argument about doubling M, we get a bound on the whole code.

$$E \leq \frac{s}{2} \sum_n \frac{S_n}{N_{bn}} - \frac{1}{2} \sum_n \ln \frac{N_{bn} - sN_n}{(1-s)N_{bn}} + \ln 8. \tag{56}$$

We again maximize (56) over s.

$$\frac{d}{ds} = \frac{1}{2} \sum_n \frac{S_n}{N_{bn}} - \frac{1}{2} \sum_n \frac{N_{bn} - N_n}{(1-s)(N_{bn}-sN_n)}$$

$$= \frac{1}{2} \sum_n (N_{bn}-N_n) \left[\frac{1}{(1-p)(N_{bn}-pN_n)} - \frac{1}{(1-s)(N_{bn}-sN_n)}\right] = 0.$$

This can easily be seen to be met when $s = p$. To verify that this is a maximum and the only maximum,

$$\frac{d^2}{ds^2} = -\frac{1}{2} \sum \frac{N_{bn} - sN_n + (1-s)N_n}{(1-s)^2 (N_{bn}-sN_n)^2} < 0$$

for all s between 0 and 1.

If we replace s by p in (56) we see that R determines p by (54), and p in turn determines E by (56).

When Eq. 56 is written in terms of ρ, where

$$\rho = \frac{s}{1-s},$$

we have

$$E \leqslant \frac{\rho}{2(1+\rho)} \sum_n \frac{S_n}{N_{bn}} - \frac{1}{2} \sum_n \ln \left(1+\rho-\rho \frac{N_n}{N_{bn}}\right) + \ln 8. \tag{57}$$

We now undertake to show that maximization of Eq. 57 over the signal power distribution results in (47) (the sphere-packing bound) and, further, that any other signal distribution will have an inferior exponent. Equation 57 must be maximized, subject to the constraint

$$S = \sum_n S_n = \text{constant}.$$

This maximization can be avoided by adding ρ times the right side and substracting ρ times the left side of Eq. 54 to Eq. 57. By defining

$$r_n = \frac{\rho}{2N_{bn}(1+e)^2}$$

and using (48), after some algebraic manipulations, Eq. 57 becomes

$$E \leqslant (1+\rho) \sum_n S_n r_n + \frac{1}{2} \sum_n \ln (1-2r_nS_n) - \rho R$$

$$+ \frac{\rho}{2} \sum_n \ln \left(1-2r_nS_n + \frac{S_n}{N_n(1+\rho)}\right) + \ln 8$$

$$+ \rho \left[\frac{\epsilon}{2} + \frac{a}{2(1-a)} \sum_n \frac{S_n}{N_{bn}} + \ln \frac{4}{a\epsilon(1-a)} \sum_n \frac{S_n}{N_{bn}}\right.$$

$$\left. + 2\sqrt{\sum_n \frac{(N_{bn}-N_n)^2}{N_{bn}^2} + \sum_n \frac{S_n}{(1-a)N_{bn}}}\right]. \tag{58}$$

Before maximizing this we can bound several of the terms:

$$\sum_n \frac{S_n}{N_{bn}} \leqslant \sum_n \frac{S_n}{N_n} \leqslant \sum_n \frac{S_n}{N_{min}} = \frac{S}{N_{min}},$$

where N_{min} is the smallest value of N_n, with $S_n \neq 0$,

$$\sqrt{\sum_n \frac{(N_{bn}-N_n)^2}{N_{bn}^2} + \sum_n \frac{S_n}{(1-\alpha)N_n}} \leq \sqrt{2\frac{S}{(1-\alpha)N_{min}}},$$

and finally from (54),

$$1+\rho \leq \frac{S}{2N_{min}\left[R-\frac{\epsilon}{2}-\frac{\alpha S}{2(1-\alpha)\ N_{min}}\right]-\ln\frac{4S}{\alpha\epsilon(1-\alpha)\ N_{min}}}.$$

The terms from ln 8 on can then be bounded by functions that are independent of the distribution on S_n. The first four terms are exactly those considered in Section II, except that Q_n is replaced by S_n. There we maximized over ρ, r_n, and S_n, but here ρ and r_n are functions of S_n. Nevertheless, we can ignore this dependence and obtain a bound on E. The bound is just the lower bound to E plus the ln 8, etc. terms, and the functional relation between ρ, r_n, and S_n is correct. Therefore this distribution of S_n is optimum, and the upper bound differs from the lower bound only by the terms ln 8, etc. The solution given by the Kuhn-Tucker theorem is necessary and sufficient for a maximum; in other words, all maxima are given by the solution and, since we got only a point solution, this means that this point is the only maximum. To finish the argument we must show that the maximum over ρ also gives only a point. From Eq. 45, we calculate

$$\frac{d^2E}{d\rho^2} = \frac{1}{2}\sum_{n_o} \frac{1}{N_b}\frac{dN_b}{d\rho} \neq 0,$$

which shows that the maximum is a point.

We have shown that any power distribution, S_n, which is not identical to the optimum distribution on Q_n derived in Section II will result in an inferior exponent, E, with the ln 8, etc. terms neglected. A more important question is, What happens to the "exponent"?

$$\lim_{T\to\infty} -\frac{\ln P_e}{T} = \lim_{T\to\infty}\frac{E}{T}?$$

It is clear that having the "incorrect" energy in a finite number of the S_n is not going to affect the limit, as long as the great majority of the S_n are correct, but the limit will be weakened if a nonvanishing fraction of the S_n do not approach Q_n in the limit as $T \to \infty$. This is the case when the spectrum of the set of input code words is incorrect.

3.3 STRAIGHT-LINE BOUND

The bound that has been obtained thus far includes a term in -ln L with the rate. This represents a decoder that forms a list of L outputs rather than guessing at just one. The purpose of including this term is to form a foundation upon which a tighter lower bound can be built. We are free to break the set of parallel or eigenfunction channels up into two groups and then use a theorem of Gallager[21]:

Let $P_1(B_1, M, L)$ be a lower bound on the average probability of error for list decoding with code words used with probability P(m), and transmitted over a set of parallel channels denoted B_1. Let $P_2\left(B_2, \frac{L}{2}\right)$ be a lower bound on the probability of decoding error for at least one word in any code with $\frac{L}{2}$ code words transmitted over a set of parallel channels denoted B_2. Then any code with M code words used with probability P(m) using both the sets B_1 and B_2, of parallel channels, has an average probability of error:

$$P_e \geqslant \frac{P_1(B_1, M, L)\ P_2(B_2, L/2)}{4}. \tag{59}$$

This theorem is proved in Appendix D.

The splitting of the set of channels into two parts and the analysis through Eq. 57 can be applied after the code is given, since it merely bounds the probability of error and does not actually affect the decoding. Therefore one can let the way the channel is to be split depend on the code. It is difficult to analyze this problem in its full generality, so we shall consider a few special cases: a straight-line bound, an improved low-rate bound, and a proof that the sphere-packing bound does not yield the tightest possible exponent for $\rho > 1$.

In order to obtain a straight-line bound corresponding to Shannon's and Gallager's[21] bound for the discrete channel, we need to split the channel in a special way. First, we pick a rational number, q, between 0 and 1. This q represents the fraction of the parallel channels to be in set B_1; therefore (1-q) is the fraction of the channels that are in B_2. Divide the channels as follows. Pick the smallest number (V) divisible by q, then partition the set of parallel channels into groups of V per group, starting with the parallel channel with the smallest N_n and working up. Therefore each group of V channels has somewhat the same average noise power, and as T is increased the spread of N_n within a group approaches zero. Each of these groups also has a spread of S_n, but this spread may be very large, since we have not tried to restrict it. We observe at this point that we can make

$$S_1 = \sum_{B_1} S_n \geqslant qS$$

by always putting the qV channels with larger S_n in the set B_1, or we can make

$$S_1 \leqslant qS$$

by always putting the qV channels with smaller S_n in the set B_1; which of these we shall do will depend on the other parameters, but we do have the choice of doing either. With either of the foregoing divisions of the channels we can write for any positive number ϵ and T large enough,

$$\sum_{n_o \cap B_1} \ln \frac{N_b}{N_n} = q \sum_{n_o} \ln \frac{N_b}{N_n} \pm \epsilon T.$$

Using the sphere-packing bound for P_1 we write

$$-\ln P_1(B_1, M, L) \leq \frac{S_1}{2N_b(1+\rho)} + \frac{q}{2} \sum_{n_o} \ln \left(1 + \rho - \rho \frac{N_n}{N_b}\right) + \epsilon T$$

when

$$R = \frac{q}{2} \sum_{n_o} \ln \frac{N_b}{N_n} + \epsilon T.$$

Here, we have included all of the "small" terms in ϵT, which will cover them all for large enough T and small enough α.

For P_2 we shall make use of an asymptotic bound at zero rate given by Shannon.[20] He showed that for a channel disturbed by white Gaussian noise,

$$P_e \geq \exp\left(-\frac{S}{4N_o} - \epsilon T\right)$$

for any positive ϵ, provided that M be equal to or greater than some M_ϵ and T larger than some T_ϵ. Certainly, one cannot do better in colored Gaussian noise if $N_{min} = N_o$, and thus we have

$$E(0) \leq \frac{S}{4N_{min}} + \epsilon T.$$

Equation 59 becomes

$$-\ln P_e \leq \ln 4 + \frac{\rho S_1}{2N_b(1+\rho)} + \frac{q}{2} \sum_{n_o} \ln \left(1 + \rho - \rho \frac{N_n}{N_b}\right) + \frac{S - S_1}{4N_{min}} + 2\epsilon T \tag{60}$$

for

$$R = \frac{q}{2} \sum_{n_o} \ln \frac{N_b}{N_n} + \epsilon T. \tag{61}$$

We have chosen L to be $2M_\epsilon$ so that ln L will not grow with T. Equation 60 can be written

$$-\ln P_e \leqslant \ln 4 + S_1\left(\frac{\rho}{2N_b(1+\rho)} - \frac{1}{4N_{min}}\right) + \frac{S}{4N_{min}} + \frac{q}{2}\sum_{n_o} \ln \left(1+\rho-\rho\frac{N_n}{N_b}\right) + 2\epsilon T.$$

The multiplier of S_1 will be either positive, zero or negative. Accordingly, we restrict S_1 to be either less or greater than qS, and then

$$-\ln P_e \leqslant \frac{(1-q)S}{4N_{min}} + \frac{qS\rho}{2N_b(1+\rho)} + \frac{q}{2}\sum_{n_o} \ln \left(1+\rho-\rho\frac{N_n}{N_b}\right) + 2\epsilon T + \ln 4. \tag{62}$$

Since (61) and (62) are both linear in q, the bound is nothing more than a straight line between E(0) and a point on the sphere-packing curve given by ρ and N_b. It stands to reason that we want to make this straight line as low as possible and thus choose the point on the sphere-packing bound which produces a straight line tangent to the sphere-packing curve. This, then, is the same result obtained by Shannon and Gallager for the channel.

There are several slight improvements that can be made in this bound, although it is unlikely that any of them represents the lowest obtainable upper bounds. First, Wyner[26] has shown that the white Gaussian noise channel has an asymptotic bound given by

$$P_e \geqslant \exp\left(-\frac{TPe^{-2r}}{4N_o} - \epsilon T\right)$$

for any positive ϵ when T is greater than some T_ϵ. His bound is for a time-discrete channel with additive Gaussian noise with variance N_o and average transmitter power of P. The value r is the rate per channel use. We use this bound by replacing TP with S and determining the over-all rate by multiplying r times the number of channels in the set B_2, $\mathscr{N}(B_2)$.

$$\ln\frac{L}{2} = r\mathscr{N}(B_2).$$

If we use N_{min} instead of N_o, the bound clearly applies also to colored Gaussian noise. If we want to get any improvement over Shannon's zero rate bound, we must not let r go to zero. This can be done by making $\mathscr{N}(B_2)$ and $\ln\frac{L}{2}$ both grow linearly with T. Then r is independent of T, since it is the ratio of these numbers. In order to keep $\mathscr{N}(B_2)$ from getting too large, we put all channels with $N_n > N_b$ into the set B_1, then split the channels with $N_n \leqslant N_b$ as before (q into B, (1–q) into B_2); the only difference now is that we can only guarantee that

$$S_1 \geqslant qS,$$

since these channels with $N_n > N_b$ may have had some energy. Equation 60 now becomes

$$-\ln P_e \leqslant S_1\left(\frac{\rho}{2(1+\rho)N_b} - \frac{e^{-2r}}{4N_{min}}\right) + \frac{S\,e^{-2r}}{4N_{min}}$$

$$-\frac{q}{2}\sum_{n_o} \ln\left(1+\rho-\rho\frac{N_n}{N_b}\right) + \ln 4 + 2\epsilon T \tag{63}$$

when

$$R = \frac{q}{2}\sum_{n_o} \ln\frac{N_b}{N_n} + \ln L = \frac{q}{2}\sum_{n_o} \ln\frac{N_b}{N_n} + (1-q)\left(\sum_{n_o} r + \ln 2\right) + \epsilon T.$$

If the multiplier of S_1 is negative, we can overbound the right side of (63) by letting $S_1 =$ qS.

$$-\ln P_e \leqslant \frac{qS\rho}{2(1+\rho)N_b} - \frac{q}{2}\sum_{n_o} \ln\left(1+\rho-\rho\frac{N_n}{N_b}\right) + \frac{(1-q)\,e^{-2r}}{4N_{min}} + 2\epsilon T,$$

which is just our straight line again, only now it is drawn between the sphere-packing bound and the Wyner bound given by

$$E = \frac{S\,e^{-2r}}{4N_{min}}$$

$$R = \sum_{n_o} r + \ln 2. \tag{64}$$

E and R are functions of the parameters r and N_b, subject to the restriction that the multiplier of S_1 in (63) be negative, or

$$r \leqslant \frac{1}{2}\ln\frac{(1+\rho)N_b}{2\rho N_{min}}. \tag{65}$$

In other words, the straight line can only be drawn for r satisfying (65). If Eq. 65 requires r to be less than zero, Eqs. 64 are useless.

Finally, we shall look at the bound when the signal power distribution is known. We can find the best way to split up the channel into a sphere-packing part and zero-rate part, the means depending only on the signal-to-noise ratio in the component channels.

The zero-rate bound for a known signal power distribution is given by an expression of Berlekamp[1] for the discrete memoryless channel:

$$E(0) = -\min_{P(\underline{x})} \sum_{\underline{x}_1} \sum_{\underline{x}_2} P(\underline{x}_1)\, P(\underline{x}_2) \ln \sum_{\underline{y}} \sqrt{P\left(\frac{\underline{y}}{\underline{x}_1}\right) P\left(\frac{\underline{y}}{\underline{x}_2}\right)},$$

where x_1 and x_2 range over the entire input space and are distributed according to $P(\underline{x})$, and $\underline{y}$ ranges over the entire output space. This can be extended to the Gaussian noise case and the evaluation gives

$$E(0) = \frac{1}{4} \sum_n \frac{S_n}{N_n}$$

which depends only on the signal-to-noise ratio. The sphere-packing bound was shown in section 3.2 to be

$$E = \frac{\rho}{2(1+\rho)} \sum_n \frac{S_n}{N_n} - \frac{1}{2} \sum_n \ln \left(1 + \rho - \rho \frac{N_n}{N_{bn}}\right) + \epsilon T$$

$$R = \frac{1}{2} \sum_n \ln \frac{N_{bn}}{N_n} + \epsilon T,$$

where $\frac{N_{bn}}{N_n}$ is a function of $\frac{S_n}{N_n}$, given by

$$\frac{S_n}{N_n} = (1+\rho)^2 \frac{\frac{N_{bn}}{N_n} - 1}{1 + \rho - \rho \frac{N_n}{N_{bn}}}, \qquad \frac{N_{bn}}{N_n} \geq 1.$$

Therefore this exponent is again dependent only on the ratio S_n/N_n.

Clearly, if there is to be any division of the component channels between the zero-rate and sphere-packing portions, it must be done on the basis of S_n/N_n. One possible division is to pick some threshold signal-to-noise ratio and put all of those channels with signal-to-noise ratio less than the threshold into the zero-rate portion and all with signal-to-noise ratio larger than the threshold into the sphere-packing portion.

This approach has, thus far, been intractable and has only yielded the one small bit of insight that the sphere-packing exponent cannot be attained for $\rho > 1$, for any channel with differentiable noise power density spectrum. We have shown that there is only one power distribution that achieves the sphere-packing bound for $\rho \leq L$; any other power distribution produces an inferior bound. We now take the channels and split them up by an arbitrary N_d such that for channels in B_2, $N_n > N_d$, and channels in B_1, $N_n \leq N_d$. In this case we know what S_n is, simply because the distribution must be that which gives the sphere-packing bound. We therefore chose N_d to be slightly less than N_b, thereby increasing P_1. In picking a smaller energy for the sphere-packing part we must have a larger P_1 because we know that for this particular bound

$$\frac{\partial E}{\partial S} = \frac{\rho}{2(1+\rho)N_b}. \tag{66}$$

The fact that the channel over which we must transmit is now slightly inferior can only make the loss greater. Some of the loss in exponent is brought back by the zero-rate exponent, and this amount is given by

$$\frac{\partial E_2}{\partial S} = \frac{1}{4N_d}. \tag{67}$$

Clearly, when (66) is larger than (67) we shall have a net loss in exponent. If $\rho \leqslant 1$, there will never be a loss, as might be expected, since we have shown that for $\rho \leqslant 1$ the value of E is both an upper and a lower bound. For $\rho > 1$ there will always be some $N_d < N_b$ that will produce a loss. N_d must be chosen very close to N_b, since Eq. 66 has a positive second derivative and therefore can only be used as a linear approximation for very small variations.

We have now shown that the sphere-packing bound gives the true exponential behavior for $\rho \leqslant 1$, but does not give the tightest lower bound for $\rho > 1$. There is one exception — when the noise spectrum, and subsequent signal spectrum, is such that choosing N_d slightly less than N_b produces no reduction in the set B_1. An example of this is the bandpass white Gaussian channel. All exceptions are ruled out if we insist that the noise spectrum be continuous.

3.4 NECESSARY CONSTRAINTS ON SIGNALS

We are now in a better position to comment on the kind of signals needed to communicate with the optimum probability of error exponent. We have shown that unless a set of signals has the given power distribution over the component channels it will be unable to achieve the optimum exponent. If the signal has the correct power distribution, it can achieve the exponent, but we have no indication whether the signals must be on the shell or not.

In any code there will be a distribution of energy over the code words. We will define $\Phi(S)$ as

$$\Phi(S) = \frac{1}{M} \text{ number of code words for which } S \geqslant |x|^2.$$

Now define R_S as the rate of the code consisting of all the code words with energy $\leqslant S$:

$$R_S = \ln M\Phi(S) = R + \ln \Phi(S).$$

We claim that for the original code,

$$P_e \geq \Phi(S)\, e^{-E_S(R_S)} \tag{68}$$

for any $0 \leq S \leq \infty$, where $E_s(R_S)$ is the lower-bound exponent calculated in Section III. The proof of this is obvious; we simply have a subset of the code with $M\Phi(S)$ code words, all with energy equal to or less than S, and this subset is used $\Phi(S)$ of the time.

Suppose the code is an optimum code, then for $R \geq R_{crit}$ we have

$$P_e \leq \exp[-E_{\bar{S}}(R)+\epsilon T], \tag{69}$$

where $\epsilon > 0$ can be made as small as one likes by making T sufficiently large, and $E_{\bar{S}}(R)$ is the same as the lower-bound exponent. Then using (68) and (69), we have

$$E_{\bar{S}}(R) - E_S(R_S) \geq \ln \Phi(S) - \epsilon T. \tag{70}$$

Because of the convexity of E(R) in both S and R, we can write

$$E_{\bar{S}}(R) \geq E_S(R) + \frac{\rho}{2N_b(1+\rho)} (\bar{S}-S)$$

and

$$E_S(R) \geq E_S(R_S) + \rho' \ln \Phi(S).$$

Thus we write (70)

$$-(\bar{S}-S) \frac{\rho}{2N_b(1+\rho)} - \rho' \ln \Phi(S) \geq \ln \Phi(S) - \epsilon T$$

or

$$\ln \Phi(S) \leq -(\bar{S}-S) \frac{\rho}{2N_b(1+\rho)(1+\rho')} + \frac{\epsilon T}{1+\rho'}.$$

Since ϵ can be made arbitrarily small and S is linear in T, the second term on the right is of no consequence. The first term on the right is $\bar{S} - S$ multiplied by a nonzero negative constant; consequently, $\Phi(S)$ must fall off at least exponentially below $\bar{S}$ with a rate of decay that is independent of T for fixed $\bar{S}/T$. There are certain ensembles of random codes for which one cannot expect this exponential behavior. If, for example, the ensemble is defined by choosing the coordinates of $\underline{x}$ independently, one finds that the distribution function of S does not fall off exponentially near $\bar{S}$, but falls off as $e^{-\alpha(\bar{S}-S)^2/T}$, α a positive constant. Then as T gets larger with fixed $\bar{S}/T$ and fixed $(\bar{\bar{S}}-S)$, the distribution function with independent components must approach 1/2, and cannot correspond to the optimum distribution, as seen in Fig. 8. This does not imply that none of the codes in the ensemble has the optimum exponent (certainly some of them do),

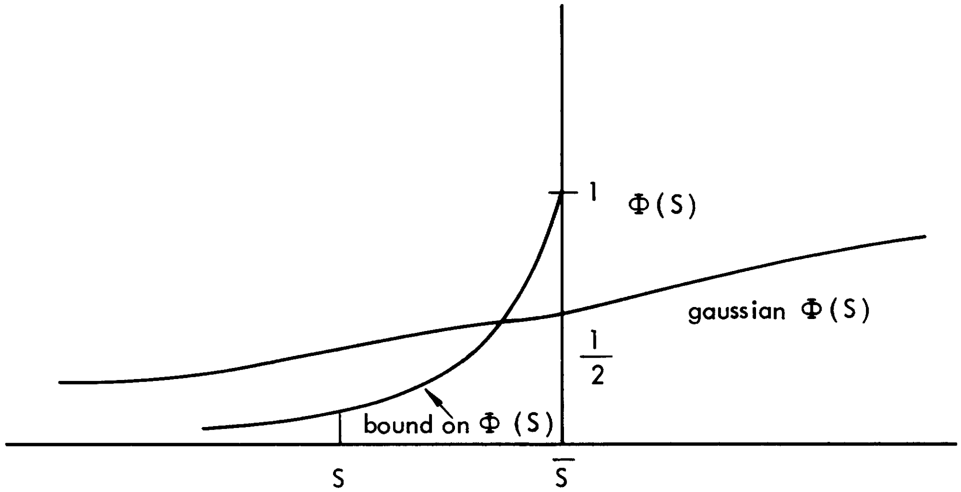


Fig. 8. Exponential bound on $\Phi(S)$ and Gaussian $\Phi(S)$.

but it implies that the ensemble behavior is not optimum and that the poorer codes, with somewhat weaker exponential behavior than optimum codes, dominate the ensemble behavior.

Now that we have found out what ensembles have poor average P_e, a comment is in order about what ensembles besides the shell distribution have optimum exponential behavior. In Section II we bounded the shell distribution by a function $w(\underline{x})$ and obtained an optimum exponent. Consequently, any $P(\underline{x}) \leq w(\underline{x})$ will produce an ensemble of codes with the optimum exponent.

IV. VARIABLE BLOCKLENGTHS

We shall now allow ourselves the freedom to use separate coders and decoders for the individual parallel channels. Until now the parallel-channel problem has been considered in the context of coding with a fixed blocklength over the product alphabet which is formed by taking all combinations of one symbol from each of the parallel channels. This problem is well defined without reference to any particular coding and decoding system, since the blocklength is fixed; how one is to go about building a system with the given blocklength is a separate problem. The composite-channel problem has been solved by Gallager.[8] He found that the reliability function for any discrete memoryless channel is given by

$$E(R) = \max_{\rho} E_o(\rho) - \rho R, \tag{71}$$

where

$$E_o(\rho) = -\ln \sum_{\underline{y}} \left(\sum_{\underline{x}} p(\underline{x})\, p(\underline{y}/\underline{x})^{1/(1+\rho)} \right)^{1+\rho}.$$

Equation 71 is usually maximized with respect to ρ by setting the derivative with respect to ρ equal to zero. Thus

$$R = \frac{\partial E_o(\rho)}{\partial \rho}. \tag{72}$$

If we substitute (72) back in (71), we obtain parametric expressions for E and R in terms of ρ. The parametric expressions fail to give the true $E(R)$ only when the $E(R)$ curve has discontinuities of slope, in which case one must ignore a range of ρ, that is, the parametric expressions double back on themselves and are thus superfluous over a range of ρ.

A composite channel C, made up of channels A and B in parallel, has an $E_{o_C}(\rho)$ given by

$$E_{o_C}(\rho) = E_{o_A}(\rho) + E_{o_B}(\rho).$$

Equation 71 becomes

$$E_C(R) = \max_{\rho} \left[E_{o_A}(\rho) + E_{o_B}(\rho) - \rho R\right]. \tag{73}$$

Taking the derivative with respect to ρ and setting it equal to zero gives

$$R = \frac{\partial E_{oA}(\rho)}{\partial \rho} + \frac{\partial E_{oB}(\rho)}{\partial \rho}. \tag{74}$$

We observe that R is the sum of the parametric expressions for rate on channels A and B; consequently, when (74) is substituted in (73), Eq. 73 is the sum of the parametric expressions for E on channels A and B.

We therefore obtain the parametric expressions for the composite channel from

$$E_c(\rho) = E_A(\rho) + E_B(\rho)$$

$$R_c(\rho) = R_A(\rho) + R_B(\rho).$$

When either channel A or B, or both, has parametric expressions that double back on themselves, the parametric expressions for the composite channel may also do so, but the true value of E(R) can be found by again ignoring the superfluous part of the parametric expressions.

One can see that, for any rate, the composite channel always has a larger E(R) than either parallel channel. One might wonder why we would ever want to use separate coder-decoders, since we must always use much larger blocklengths on both parallel channels than we would have to use on the composite channel to obtain a given P_e. In order to see that separate coding is a reasonable possibility, we consider the example of two identical channels in parallel. These two channels have the same input and output alphabets and the same transition probabilities. Consequently, it does not matter through which channel any given letter is sent. Suppose a coder-decoder of blocklength N and rate R has been designed to work on the composite channel. Instead of transmitting the signals through the parallel channels in the normal manner, we can take the first block of signals and send it all through channel A. We send the normal signal for the first N transmissions, then send the signal that would otherwise have gone over channel B during the second N transmissions, thereby using up 2N transmissions. The received signal can be decoded in the normal manner by waiting for the 2N transmissions and treating the second N transmissions as if they had come over channel B. We have reduced our information rate by 1/2, but this can be made up by sending the alternate blocks on channel B. The coder and decoder will not have to operate any faster, since we are operating at the same total information rate as before. Consequently, we have managed to change from composite coding to separate coding and decoding on each channel without changing either the P_e or the amount of equipment needed. We have doubled the blocklength in the change, but this increase cost us nothing in terms of equipment. It is therefore just as reasonable, in this case, to use separate coding as composite coding.

When one introduces the freedom to have separate coder-decoders on the parallel channels one must be willing to admit the possibility of using different blocklengths on the parallel channels. Consequently, a new constraint must replace the fixed blocklength constraint used previously. A logical parameter to constrain would be cost, since, in practice, this is usually what prevents the use of large blocklengths. In order to constrain cost we must have some reasonable way to measure the cost which will not vary from day to day as the price of computers varies. For these reasons, we shall use a quantity that we call "complexity"; it is defined as the number of logical operations needed per second to perform the coding and decoding. This is generally the cost parameter used in evaluating coding and decoding schemes. Complexity, then, is a function of the channel, the coding-decoding scheme, the rate, and the blocklength; consequently, we write

$$D = D_A(R_A, N_A),$$

where the subscript A means channel A with its associated coding-decoding scheme.

One is free to weigh the various logical operations in order to bring complexity more in line with cost. For example, a multiply could be considered as 10 logical operations, and an add as one. If storage is a significant part of the coder-decoder, one could include it in the complexity.

We are now in a position to state the basic questions. When one has several parallel channels and is willing to use a certain total amount of complexity in all coder-decoders, What is the smallest P_e attainable and how does one go about obtaining it? Does one use composite coding over the product alphabets, or does one use separate coders on the parallel channels? If one uses separate coders, how is the rate divided between then and what blocklength is used for each coder-decoder? It is only fair to say at the beginning that we do not solve these problems, but we do achieve guides to what the solutions may be, and in some cases we are able to show an improvement over the previous results with composite coding.

For the sake of mathematical convenience, we shall state the problem slightly differently. If one is to obtain a given P_e at a given rate, what is the minimum total complexity that is needed, and how does one decide what rates and blocklengths to use? The questions are identical to the previous ones, if one assumes that the complexity required increases as P_e decreases. This is an underlying assumption of the whole problem, anyway.

In addition to finding the appropriate choice of rates and blocklengths on the parallel channels, one may have various other parameters at one's disposal. One such example is the choice of power to be used on each channel where the over-all power is constrained. We shall consider this case later on, for the channel with additive Gaussian noise.

Most of the results obtained here are asymptotic. This is primarily due to the difficulty of obtaining anything but asymptotic results. To get results for small blocklengths, one must tabulate the performance of a number of known codes. This approach is inherently limited by the number of codes that can be tabulated. On the other hand, the asymptotic results are a great deal more general, and tend to make the relationships between the various parameters clear. The results of Sections I and II are asymptotic, as is the whole idea behind the reliability function.

We shall be primarily interested in the way in which the complexity function increases with N for large N. For practical considerations, we can ignore those coding schemes in which complexity increases with N faster than N to some small power. If the complexity increases too fast with blocklength, the price for high reliability transmission will be too large to be interesting. In particular, this rules out those complexity functions that are exponential in N, and therefore we can be assured that

$$\lim_{N\to\infty} \frac{\ln D(R,N)}{N} = 0$$

for all channels at rates less than capacity.

Complexity must also increase with rate; if not, one could transmit at larger rate and then throw away some of the information to effect a net gain. If there is a power consideration, one can see that complexity must decrease with power, otherwise one could just as well throw away some of the power at the transmitter. It might be argued that as the rate increases above capacity the complexity can be made zero, since it is impossible to decode correctly, anyway. This argument is negated by our fixing P_e at some small value and then varying the remaining parameters.

We shall examine the over-all problem in small pieces, in order to get some insight into what is happening at each stage. This approach is needed here because we are not able to get any general solutions. We do get some asymptotic results (asymptotic in blocklength) and solutions for some assumed complexity functions.

4.1 DETERMINATION OF BLOCKLENGTHS

To begin, we shall assume that separate coding is to be used for the parallel channels, the channels are fixed, and the rates for each channel, R_A and R_B, have already been chosen. All that we have to do is find the choice of N_A and N_B which minimizes the complexity for a fixed P_e.

For each of the parallel channels we know that

$$P_e \leq e^{-N[E(R)-\epsilon_N]},$$

where ϵ_N is zero for the discrete constant channel and approaches zero as N approaches ∞ for Gaussian noise channels. For small N, ϵ_N may be quite large.

The average P_e for the two parallel channels is bounded by

$$P_e \leq \frac{R_A}{R} e^{-N_A E_A(R_A)+N_A\epsilon_{N_A}} + \frac{R_B}{R} e^{-N_B E_B(R_B)+N_B\epsilon_{N_B}}. \tag{75}$$

This bound is asymptotically correct when E(R) is the tightest possible reliability function. We observe from Eq. (75) that there is no point to making the P_e on one of the parallel channels significantly lower than that on the other. To do so would not change the bound on P_e much and would only waste complexity in the coder-decoder. For very large blocklength, when (75) is tight, a good approximation of (75) is given by

$$P_e \leq e^{-N_m E_m(R_m)+\epsilon N_m}, \tag{76}$$

where

$$N_m E_m(R_m) = \min \begin{cases} N_A E_A(R_A) \\ N_B E_B(R_B), \end{cases}$$

and ϵ is a positive number that goes to 0 as the blocklength increases. If we ignore the ϵ, we shall minimize the complexity for a fixed P_e by letting

$$N_A E_A(R_A) = N_B E_B(R_B) = \text{constant}, \tag{77}$$

where the constant is chosen to obtain the desired over-all P_e, and is approximately $-\ln P_e$.

4.2 DETERMINATION OF RATES

We now consider the next step in the problem, that of choosing the rates for channels A and B. Let us assume that separate coding is to be used and the channels are fixed. Equation (77) gives N_A implicitly as a function of R_A for a fixed value of P_e, and also N_B as a function of R_B. Consequently, as we vary R_A and R_B the blocklengths will also vary to meet (77) with a fixed P_e. From (77), the variation in N_A with respect to the variation in R_A is

$$\frac{dN_A}{dR_A} = -\frac{N_A}{E_A(R_A)} \frac{dE_A(R_A)}{dR_A} = \frac{\rho_A N_A}{E_A(R_A)}.$$

Likewise, we find

$$\frac{dN_B}{dR_B} = \frac{\rho_B N_B}{E_B(R_B)}.$$

R_A and R_B are not independent variables, since we must keep $R_A + R_B = R$ a constant. Therefore the variation of R_B with respect to R_A is -1. This leaves us with R_A as the only free variable, so all that we have to do is set the variation in complexity with respect to R_A equal to zero. The complexity is given by

$$D = D_A(R_A, N_A) + D_B(R_B, N_B).$$

We wish to minimize D by setting the total derivative of it with respect to R equal to 0; this is done by taking the partial derivatives with respect to R_A, R_B, N_A, and N_B and multiplying each partial derivative by the variation of that parameter with respect to R_A. We have

$$\frac{\partial D_A(R_A, N_A)}{\partial R_A} - \frac{\partial D_B(R_B, N_B)}{\partial R_B} + \frac{\partial D_A(R_A, N_A)}{\partial N_A} \frac{\rho_A N_A}{E_A(R_A)} - \frac{\partial D_B(R_B, N_B)}{\partial N_B} \frac{\rho_B N_B}{E_B(R_B)} = 0. \tag{78}$$

This cannot be solved without some additional knowledge of the nature of the complexity functions. In order to get some idea of how the rates must be chosen, we shall look at some examples of complexity functions. Let the complexity be given by

$$D_i(R_i, N_i) = \alpha_i(R_i)\, N_i^{\beta_i(R_i)}.$$

This is a fairly general expression and it covers most known coding schemes.

$$\frac{\partial D_i(R_i, N_i)}{\partial R_i} = \alpha_i'(R_i)\, N_i^{\beta_i(R_i)} + \alpha_i(R_i)\, N_i^{\beta_i(R_i)} (\ln N_i \beta_i'(R_i))$$

$$\frac{\partial D_i(R_i, N_i)}{\partial N_i} = \frac{\alpha_i(R_i)\, \beta_i(R_i)\, N_i^{\beta_i(R_i)}}{N_i}.$$

Therefore Eq. (78) becomes

$$N_A^{\beta_A(R_B)} \left(\alpha_A'(R_A) + \alpha_A(R_A)\, \beta_A'(R_A) \ln N_A + \frac{\alpha_A(R_A)\, \beta_A(R_A)\, \rho_A}{E_A(R_A)} \right)$$

$$= N_B^{\beta_B(R_B)} \left(\alpha_B'(R_B) + \alpha_B(R_B)\, \beta_B'(R_B) \ln N_B + \frac{\alpha_B(R_B)\, \beta_B(R_B)\, \rho_B}{E_B(R_B)} \right). \tag{79}$$

We can see what the asymptotic solution is by observing that as N_A and N_B get larger one cannot meet (79), unless either $\beta_A(R_A) \to \beta_B(R_B)$ or one of $E_A(R_A)$ or $E_B(R_B) \to 0$. The requirement that $D_i(R_i, N_i)$ must increase with increasing R_i implies that $\beta_i(R_i)$ increases with R_i. When β is strictly increasing with increasing R_i there can be only one choice of R_A and R_B for which

$$R_A + R_B = R,$$

and

$$\beta_A(R_A) = \beta_B(R_B).$$

The case in which $\beta_i(R_i)$ is constant over some range of R_i is similar to the constant-β case which will be considered later. If one of the exponents approaches zero we must use one channel very near capacity. This only happens when one channel is much easier to code for than the other, even near capacity.

If one sets $\beta_A(R_A) = \beta_B(R_B)$ and then calculates the total complexity, one has

$$D = \alpha_A(R_A)\, N_A^{\beta_A(R_A)} + \alpha_B(R_B)\, N_B^{\beta_B(R_B)}$$

$$= \left\{ \alpha_A(R_A) + \alpha_B(R_B) \left(\frac{E_A(R_A)}{E_B(R_B)} \right)^{\beta_A(R_A)} \right\} N_A^{\beta_A(R_A)}.$$

We can now calculate an asymptotic relation between complexity and P_e. Using

$$P_e = e^{-N_A E_A(R_A)},$$

we have

$$D \xrightarrow[N_A \to \infty]{} \left(\frac{\alpha_A(R_A)}{E_A(R_A)^{\beta_A(R_A)}} + \frac{\alpha_B(R_B)}{E_B(R_B)^{\beta_A(R_A)}} \right) (-\ln P_e)^{\beta_A(R_A)}.$$

We compare this to a similar expression for composite coding. Using

$$P_e = e^{-N_c E_c(R_c)},$$

we have

$$D \xrightarrow[N_c \to \infty]{} \alpha_c(R_c) \left(\frac{-\ln P_e}{E_c(R_c)} \right)^{\beta_c(R_c)}$$

We can see that the primary factor determining whether or not separate coding of composite coding is asymptotically more complex is $\beta(R)$. If $\beta_c(R_c)$ is larger than $\beta_A(R_A)$, then one should use separate coding for very small P_e. If $\beta_c(R_c)$ is smaller, one should use composite coding. If $\beta_c(R_c) = \beta_A(R_A)$, one must look at the $\alpha(R)$ function to determine which alternative has the lesser complexity.

Although the complexity function mentioned above leads to a simple solution, in most known coding schemes $\beta(R)$ is a constant, independent of R. It is instructive to note that different coding schemes have different powers of N in the complexity function. Besides the obvious observation that it is best to use a scheme with a small power if one is going to require a small P_e, we can observe that if coding for the composite channel requires a scheme with a large power of N than coding on the channels separately, one should code separately.

There is sometimes another reason for coding separately. The transition probabilities of the separate channel are much more likely to be symmetrical than those of the composite channel. Consequently, the separate channels are more suitable for known algebraic codes such as the Bose-Chaudhuri or Reed-Solomon[15] codes.

To examine the case in which $\beta(R)$ is a constant, we let

$$D_i(R_i, N_i) = \alpha_i(R_i)\, N_i^{\beta},$$

Now Eq. 38 becomes

$$N_A^{\beta}\left(\alpha'_A(R_A) + \frac{\alpha_A(R_A)\,\beta\rho_A}{E_A(R_A)}\right) = N_B^{\beta}\left(\alpha'_B(R_B) + \frac{\alpha_B(R_B)\beta\rho_B}{E_B(R_B)}\right).$$

The asymptotic solution to this is

$$\frac{\alpha'_A(R_A)}{E_A(R_A)} + \frac{\alpha_A(R_A)\,\beta\rho_A}{E_A(R_A)^{1+\beta}} = \frac{\alpha'_B(R_B)}{E_B(R_B)} + \frac{\alpha_B(R_B)\,\beta\rho_B}{E_B(R_B)^{1+\beta}}.$$

This is about as far as we can go in this case. It is difficult to make a comparison with the composite coding case here without knowing the various $\alpha(R)$ functions.

One property of the asymptotic solution can be pointed out. When a complexity is a sum of several terms, each a power of N, the term with the highest power of N is the only important one. For example, if

$$D_A(R_A, N_A) = \alpha_A(R_A)\, N_A^{\beta} + \gamma_A(R_A)\, N_A^{q}, \qquad \beta > q$$

the only part of the complexity function that plays a part in the asymptotic solution is that term with the largest power,

$$\alpha_A(R_A)\, N_A^{\beta}.$$

This can be seen because

$$\frac{\partial D_A(R_A, N_A)}{\partial R_A} = \alpha'_A(R_A)\, N_A^{\beta} + \gamma'_A(R_A)\, N_A^{q},$$

$$\frac{\partial D_A(R_A, N_A)}{\partial N_A} = \beta\alpha_A(R_A)\, N_A^{\beta-1} + q\gamma_A(R_A)\, N_A^{q-1}.$$

In both expressions the second term is insignificant relative to the first.

4.3 DETERMINATION OF POWER DISTRIBUTION

Up to now we have assumed that the parallel channels have been fixed. It is possible that the transition probabilities could, to a certain extent, be under the control of the designer. The channels could have additive Gaussian noise with an average total power constraint. This leads to another degree of freedom in the optimization procedure. The problem can be set up in much the same way as the rate variation was. We rewrite (77) to include the power dependencies:

$$N_A E_A(R_A, P_A) = N_B E_B(R_B, P_B) = \text{constant}. \tag{80}$$

As P_A varies, N_A must vary to meet (80) and we can calculate the variation in N_A with respect to the variation in P_A as

$$\frac{dN_A}{dP_A} = -\frac{N_A}{E_A(R_A, P_A)} \frac{dE_A(R_A, P_A)}{dP_A}.$$

The quantity $\frac{dE_A(R_A, P_A)}{dP_A}$ is given in Section II. The same thing is true for channel B

$$\frac{dN_B}{dP_B} = -\frac{N_B}{E_B(R_B, P_B)} \frac{dE_B(R_B, P_B)}{dP_B}.$$

Since $P_A + P_B = P$, a constant, the variation in P_B with respect to P_A is -1. We now write the variation in total complexity with respect to variations in P_A and set it equal to zero, just as we did for rate

$$\frac{\partial D_A(R_A, N_A, P_A)}{\partial P_A} - \frac{\partial D_B(R_B, N_B, P_B)}{\partial P_B} - \frac{\partial D_A(R_A, N_A, P_A)}{\partial N_A} \frac{N_A}{E_A(R_A, P_A)}$$

$$\frac{dE_A(R_A, P_A)}{dP_A} + \frac{\partial D_B(R_B, N_B, P_B)}{\partial N_B} \frac{N_B}{E_B(R_B, P_B)} \frac{dE_B(R_B, P_B)}{dP_B} = 0. \tag{81}$$

This equation and Eq. 78 must be solved simultaneously in order to get an over-all minimum.

Almost the only interesting observation that we can make about the added freedom of power distribution is that rate and power tend to compensate for each other; once we have optimized with respect to one of the variables, optimizing with respect to the other does not reduce the complexity much more. This can be seen from the behavior of $E(R, P)$ and $D(R, N, P)$ as R and P are varied. If one is to increase R and hold $E(R, P)$ constant, one must simultaneously increase P, that is, an increase in R has the same effect on $E(R, P)$ as a decrease in P. Likewise an increase in rate has the same effect on complexity as a decrease in power. Therefore a nonoptimum power distribution can be partially compensated for by the rate distribution, and vice versa. Another way of saying this is that for fixed P_e the complexity as a function of R_A and P_A has a valley running diagonally across the R_A, P_A plane.

4.4 COMPARISON OF SEPARATE CODING TO COMPOSITE CODING

Even if we could get through the solutions of Eqs. 78 and 81, we could not be sure that we had in fact minimized the complexity. There is always the alternative of composite coding with its own complexity function. For composite coding the analysis is somewhat simpler because one can calculate the $E(R)$ function and therefore the required blocklength. All that we have to do is determine the E(R) function at the required rate. This can then be used to calculate the required N. Once R and N are determined, one can calculate $D_c(R, N)$ and compare this value with the complexity obtained by the solution of (78) and (81).

Before we go any farther, it is instructive to look at several examples of parallel channels and see what can be done with them. Let us first consider the example of two identical channels in parallel which has already been described. Here the best choice of blocklength, rate, and power is obvious. The usefulness of the example comes from the comparison of separate coding with composite coding. We have shown that in this case we could always code separately without changing either the P_e or the total complexity.

As a second example we shall take two channels that constitute an integral multiple of some base channel. Call the base channel Z, then channel A is V_A copies of channel Z in parallel, and channel B is V_B copies of channel Z in parallel. We use the same technique as in the first example. A composite coder produces a block of length N for $V_A + V_B$ copies of channel Z. We can send all of these signals over channel A in $N\left(\frac{V_A + V_B}{V_A}\right)$ transmissions. The fact that this may not be an integral number of transmissions is of no importance. It is only a matter of bookkeeping at the receiver to keep track of which signals from the various copies of Z are to be decoded as a block. On channel B we do likewise, but now require $N\left(\frac{V_A + V_B}{V_B}\right)$ transmissions. The information rate of channel A is $\frac{V_A}{V_A + V_B}$ of that on the composite channel, and the information rate of channel B is $\frac{V_B}{V_A + V_B}$ of that on the composite channel. As in the first example, we have lost no information rate, left the P_e unchanged, and used the same coder-decoder, but we have succeeded in coding for the parallel channels separately and increased the blocklength on each.

In both of these examples one quantity remained constant in going from the composite coding to the separate coding for the parallel channels. This quantity was the product of rate and blocklength. In the first example each of the parallel channels had a rate 1/2 as large as the composite channel and a blocklength twice as large. In the second example channel A has a rate $\frac{V_A}{V_A + V_B}$ of that of the composite channel and a blocklength $\frac{V_A + V_B}{V_A}$ as long; thus they have the same product of rate and blocklength. The same is true for channel B. The importance of the product rate times blocklength will become apparent when we prove a theorem concerning this product.

When the two parallel channels are not made up of several base channels, the procedure used in the examples cannot be used, but it is possible that the two channels can be transformed to bring them to a common basis. As an example of a coding scheme in which just such a transformation is part of the coder-decoder, we shall look into a scheme suggested by Forney.[7] His scheme is nonoptimum because it does not try to attain the optimum exponent but makes the probability of error small by using a larger blocklength than necessary. The advantage is that a relatively simple coder-decoder can be constructed for his large blocklength, rather than the complicated coder-decoder that is probably needed to obtain anything near the optimum exponent.

Basically, Forney's system uses two coder-decoders, an inner one that transmits and receives over the channel, and an outer one that operates on the input and output of the inner coder-decoder (see Fig. 9). The inner coder-decoder is required to produce a probability of error around 10^{-3}, have a large input-output alphabet, and have a rate

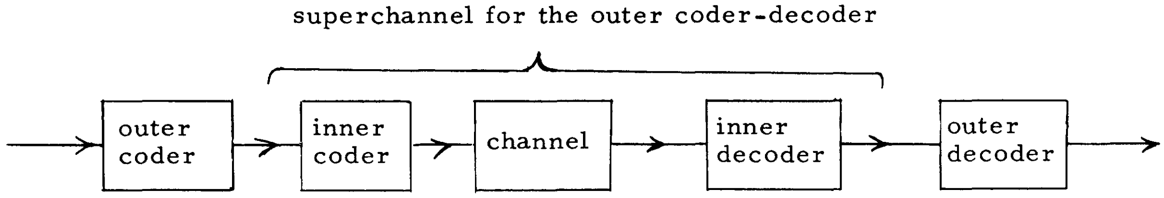


Fig. 9. Forney coding-decoding.

slightly larger than the required over-all rate. Because the P_e of the inner coder-decoder is only required to be 10^{-3}, one can design an acceptable inner system by trial and error. The outer coder-decoder uses a Reed-Solomon code with large blocklength, very small P_e, and a slight reduction of rate over the inner channel. This outer coder-decoder works over a large blocklength with a relatively simple decoding method, for which effort is proportional to some small power of N.

Forney observed that the essential purpose of the inner coder-decoder was to present a "basic" superchannel to the outer coder-decoder. This superchannel must have a probability of error around 10^{-2}-10^{-4} and sufficiently large alphabet, q, to permit the use of a Reed-Solomon code on the superchannel. The blocklength of the Reed-Solomon code is determined by the over-all P_e requirement. As the P_e requirement is lowered, the outer coder-decoder becomes the significant contributor to the complexity. This is true because the only change required of the inner coder-decoder is that its alphabet size, q, increase, which can be accomplished by taking two or more successive outputs as a single letter.

In practice one would probably build some simple system for an inner coder-decoder, since it is only required to have a P_e around 10^{-3}. In the limit, for very small P_e, the complexity of the outer coder-decoder will overshadow that of the inner system. Thus the complexity of the inner coder-decoder plays no role in asympototic results.

In order to obtain a given over-all P_e, the outer coder-decoder must see a superchannel with a $P_e \approx 10^{-3}$ and an alphabet of q. This is true whether it is going to operate on the composite channel or on the parallel channels individually. This situation corresponds to our second example; the only difference is that the parameters V_A and V_B represent the number of basic channel uses per second. The basic channels are in a sense time-parallel; channel A has $V_A = \frac{\ln q}{R_A}$ output letters per second, and channel B, $V_B = \frac{\ln q}{R_B}$. It does not matter whether the letters from the alphabet q are sent over channel A or channel B, or over a composite coder-decoder, as long as they come at a sufficiently high rate for the Reed-Solomon coder-decoder to operate at the required over-all rate, R.

When one goes from a composite system to separate systems the only change in complexity occurs in the inner coder-decoder. If one tries to find the optimum rate and power distribution, one discovers that variations in rate and power only affect the complexity of the inner coder-decoder (as long as one does not try to make the rate on one of the channels greater than its capacity). As an exercise we can assume that a maximum-likelihood coder-decoder is used as the inner system and determine the rate distribution minimizing its complexity. In this case we have

$$D_A = e^{N_A R_A},$$

$$D_B = e^{N_B R_B}.$$

This comes from the fact that the decoder must make $e^{N_A R_A}$ comparisons per block. Each comparison involves N_A letters, but we divide by N_A in order to normalize complexity to comparison per channel use. Evaluating Eq. 78, we have

$$e^{R_A N_A}\left(N_A + \frac{\rho_A R_A}{E_A(R_A)}\right) = e^{R_B N_B}\left(N_B + \frac{\rho_B R_B}{E_B(R_B)}\right).$$

We observe that $R_A N_A = R_B N_B$ is close to the solution to this equation. In particular, $\lim_{T\to\infty} \frac{R_A}{R_B} = \frac{N_B}{N_A}$ by the same argument that was used in finding the optimum blocklengths. The argument used here is an asymptotic one and, consequently, is not strictly applicable. One does not require a very long blocklength but only one large enough to achieve a $P_e \approx 10^{-3}$. The asymptotic argument was used because any nonasymptotic argument would become involved in specific codes, which we wish to avoid.

The asymptotic expression for the rate distribution of the maximum-likelihood decoder calls for a constant rate times blocklength. This is the same relationship that we observed in the two earlier examples.

We shall now prove a theorem about the attainable P_e when we code separately and select the rates by using the same rate times blocklength on both channels. We shall then investigate when the complexity function will allow us to keep rate times blocklength fixed.

Theorem: Let us code for two parallel channels with separate coder-decoders, with rates and blocklengths chosen so that P_e is the same on both channels,

$$N_A E_A(R'_A) = N_B E_B(R'_B),$$

and the information per block is the same on both channels,

$$R'_A N_A = R'_B N_B.$$

Then if we had coded for the composite channel at rate

$$R = R'_A + R'_B$$

and blocklength determined by

$$RN = R'_A N_A,$$

the P_e for the composite coding would be equal to or larger than for the separate coding,

$$NE_c(R) \leq N_A E_A(R'_A).$$

Proof: The quantities shown in Fig. 10 are

R = the over-all rate

R'_A, R'_B = the rates for the individual channels A and B

R_A, R_B = the rates that satisfy the conditions for composite coding, that is,

$$R_A(\rho) + R_B(\rho) = R_c(\rho)$$

and

$$E_A(\rho) + E_B(\rho) = E_c(\rho)$$

$$\rho = \frac{dE_A(R_A)}{dR_A} = \frac{dE_B(R_B)}{dR_B} = \frac{dE_c(R)}{dR_c}.$$

It can be seen from Fig. 10 that we have chosen R'_A and R'_B so that they add up to R, and the operating points lie on a straight line through the origin. In other words,

$$\frac{E_A(R'_A)}{R'_A} = \frac{E_B(R'_B)}{R'_B}. \tag{82}$$

The purpose for this will be seen presently. Let

$$R'_A = R_A + \Delta$$

$$R'_B = R_B - \Delta.$$

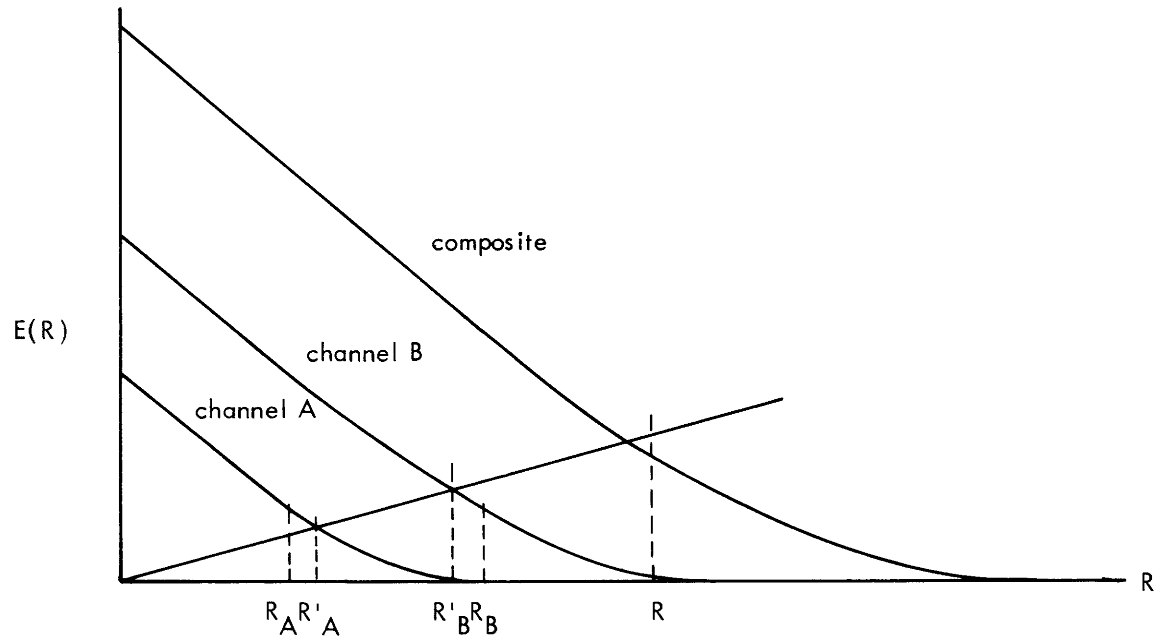


Fig. 10. Figure for Proof of the theorem.

If one takes the Taylor series expansion of $E_A(R)$ and $E_B(R)$ about the points R_A and R_B, one has

$$E_A(R'_A) = E_A(R_A) + \Delta \frac{dE_A(R_A)}{dR_A} + C_A$$

$$E_B(R'_B) = E_B(R_B) - \Delta \frac{dE_B(R_B)}{dR_B} + C_B.$$

Adding these, we have

$$E_A(R'_A) + E_B(R'_B) = E_A(R_A) + E_B(R_B) + C_A + C_B = E_c(R_c) + C_A + C_B.$$

Both C_A and C_B are positive because the E(R) functions are always convex.[8] Thus

$$E_A(R'_A) + E_B(R'_B) \geqslant E_c(R_c).$$

Dividing by $R = R'_A + R'_B$ yields

$$\frac{E_A(R'_A) + E_B(R'_B)}{R'_A + R'_B} \geqslant \frac{E_c(R_c)}{R_c}$$

or, by Eq. 82,

$$\frac{E_A(R'_A)}{R'_A} = \frac{E_B(R'_B)}{R'_B} \geqslant \frac{E_c(R_c)}{R_c}.$$

Since we held $R'_A N_A = R'_B N_B = R_c N$, we can write

$$N_A E_A(R'_A) = N_B E_B(R'_B) \geq N E_c(R_c),$$

which proves the theorem.

The theorem applies to any set of parallel channels, but it is only interesting if we can build separate coder-decoders with $R_A N_A = R_B N_B = R_c N$ without using a larger total complexity. Thus we would like to find out when

$$D_A(R_A, N_A) + D_B(R_B, N_B) \leq D_c(R_c N). \tag{83}$$

We claim that (83) will be met whenever both

$$N_A D_A(R_A, N_A) \leq N D_c(R_c, N)$$

and (84)

$$N_B D_B(R_B, N_B) \leq N D_c(R_c, N).$$

The quantity ND(R, N) is the blocklength times the number of logical operations per second, or just the number of logical operations needed to code and decode one block (under the assumption that the channel operates once per second). We define this quantity as effort, and it represents the effort needed to code and decode one block.

We prove (83) from (84) by observing that

$$D_A(R_A, N_A) \leq \frac{N}{N_A} D_c(R_c, N) = \frac{R_A}{R} D_c(R_c, N).$$

The same thing is true for channel B. Since $R_A + R_B = R_c$, Eq. 83 is met.

We shall now summarize what we have proved. Let us code for two parallel channels with the same P_e on both channels and choose the rates so that

$$R_A N_A = R_B N_B.$$

This is equivalent to choosing

$$\frac{R_A}{E_A(R_A)} = \frac{R_B}{E_B(R_B)},$$

since the P_e is the same. If we had coded for the composite channel with blocklength chosen so that

$$R_c N = R_A N_A,$$

where $R_c = R_A + R_B$, we would not be able to obtain a lower P_e. Moreover, if Eqs. 84 are met, we would not be able to accomplish the composite coding with less total complexity than we had used for separate coding.

Any coding scheme, for which the effort needed to decode a block depends only on the amount of information in the block, will meet Eq. 84 because RN is the information in a block. It is quite reasonable to expect that there will be many decoding schemes in which the effort is primarily dependent on the information content in the block.

The maximum-likelihood decoding that we considered meets (83) with equality if we add a refinement to the complexity function. We must let complexity be

$$e^{NR} \ln q$$

where q is the alphabet size. This is reasonable because the number of logical operations needed to make a comparison is proportional to the log of the alphabet size. Equation 81 becomes

$$D_A(R_A N_A) + D_B(R_B, N_B) = e^{R_A N_A} \ln q_A + e^{R_B N_B} \ln q_B = e^{R_c N_c} \ln q_c = D_c(R_c, N_c),$$

since the composite alphabet size is the product of the alphabet sizes of channels A and B.

V. SUMMARY AND SUGGESTIONS FOR FUTURE RESEARCH

In Sections II and III we considered the problem of communicating over parallel discrete time channels, disturbed by arbitrary additive Gaussian noise, with a total power constraint on the set of channels. We found explicit upper and lower bounds to the achievable probability of error with coding, which decreased exponentially with blocklength. The exponents of the upper and lower bounds agreed for rates between R_{crit} and capacity. We were also able to find the optimum signal power distribution over the parallel channels. The results were shown to be applicable to colored Gaussian noise channels with an average power constraint on the signal.

Most theoretical work on the achievable error probability with the use of coding has centered around the relationship between blocklength and error probability. Practically, one is generally more interested in the trade-off between error probability and the equipment complexity needed to implement coding. In Section IV we have investigated that relation for parallel channels and found that both error probability and complexity are parametric functions of blocklength. When the complexity is an algebraic function of the blocklength (i.e., when $D \sim N^{\beta}$) it is possible to eliminate the blocklength from the expression for P_e and express the reliability function directly in terms of complexity.

$$E(R) = \lim_{D\to\infty} \sup \frac{-\ln P_e}{D^{1/\beta}}.$$

For practical reasons, one would only be interested in building such a coder-decoder if β were small.

When a set of parallel channels all has a complexity-blocklength relation of

$$D \sim N^{\beta}$$

for the same β, then one can combine the E(R) functions of the parallel channels into a single E(R) for the parallel combination. This combined E(R) could result from an optimum choice of blocklength and rates or from some suboptimum choice. In either case, it gives a bound to P_e for a given total complexity.

$$P_e \leq e^{-D^{1/\beta}[E(r)-\epsilon]}$$

for any positive ϵ and a sufficiently large D.

The extension of this technique to channels in series seems straightforward, and, in fact, the problem is simpler because the rate must be the same on both channels.

It also appears to be a simple extension to include series combinations of channels that are themselves parallel combinations and vice versa. By this nesting of results one could reduce large networks of communication channels to a single E(R) function.

Preliminary investigation indicates that a circuit-theory analogy can be constructed in which communication links as one-way devices are analogous to one-way circuit elements. Using this analogy, one could attack the problem of non series-parallel networks. One possible approach would be to reverse the process of combination and break one of the channels up into two parallel channels. One could then split a node as shown in

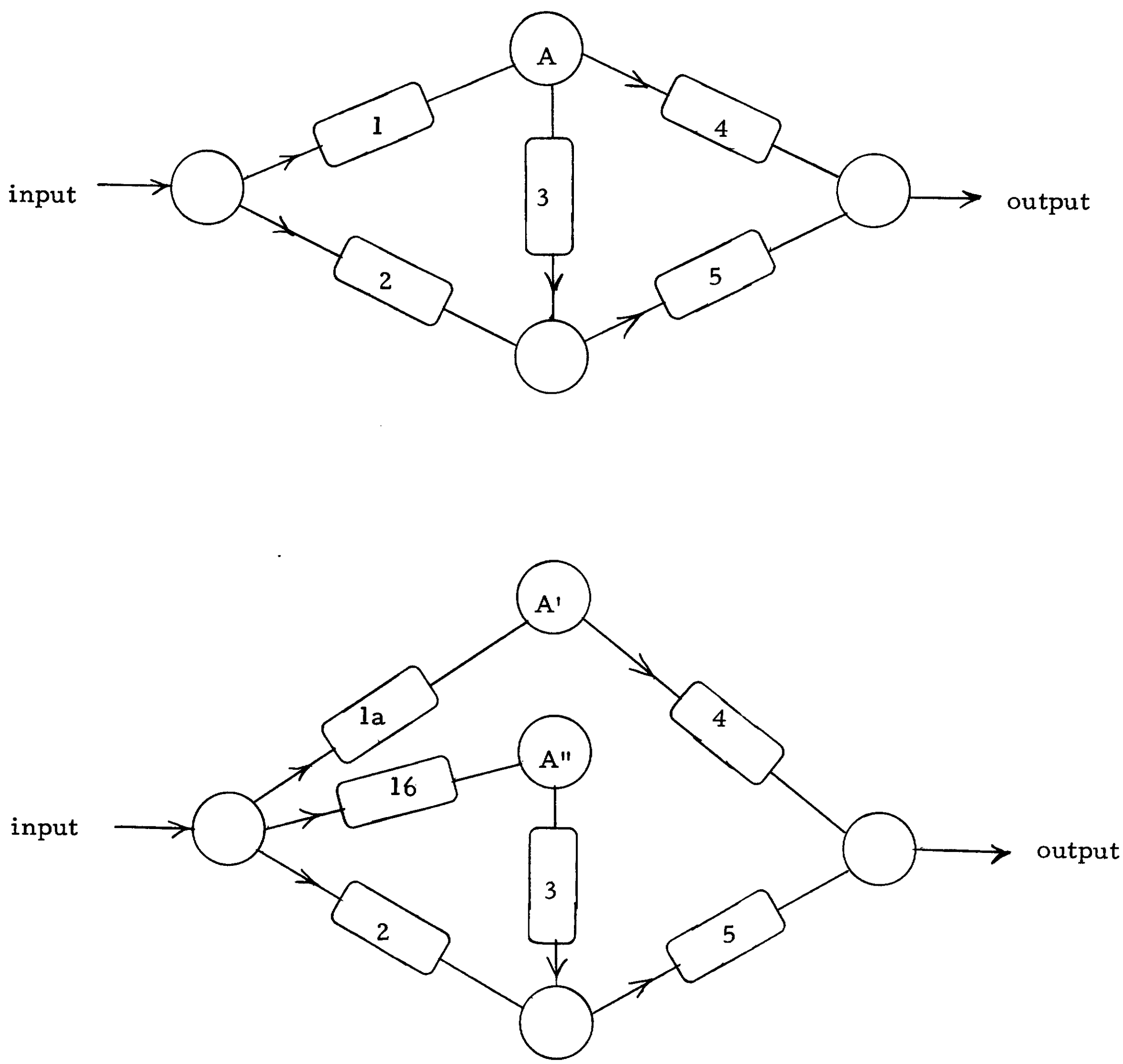


Fig. 11. Node splitting.

Fig. 11. One must require that no information would tend to flow between the halves of the node if they were connected, thus the particular way that the link is split up will depend on the over-all rate.

Finally, an extension to the case in which we have more than one information source and sink should be possible. In this case we would look for an $E(R_1, R_2, \ldots R_n)$ that would be a function of the various information rates between sources and sinks.

Care must be taken here when one uses the circuit-theory analogy because rates flowing through a link in opposite directions do not cancel as currents do. In fact, one would have to make two channels available, one operating in each direction. There would be no such problem when all information flows in the same direction.

While our results on colored Gaussian noise are considerably more complete than the results for variable blocklength, there are still several open problems here. The lower bound on P_e at low rates is not the tightest possible bound. A better minimum-distance bound would probably improve that situation considerably. Also, in all of the bounds, we have ignored coefficients and concentrated on obtaining the exponents. The coefficients become important if one wants to use the bounds at short blocklengths, and therefore it is worth while to consider them. It is possible that one could use some of the techniques of Shannon[20] on the white noise channel, since his coefficients are much tighter than ours.

The basic problem of Sections II and III is the determination of a good signal power distribution to use in coding for colored Gaussian noise channels. This problem is also met in the analysis of statistically time-variant channels. Some of the optimization techniques that we use may also be applicable to time-variant channels.

APPENDIX A

Convergence of Sum over Eigenvalues to Integral over Power Spectrum

We wish to show that

$$\lim_{T\to\infty} \sum_{n=1}^{\infty} \frac{G(N_n)}{T} = \int_{-\infty}^{\infty} G[N(w)]\, dw, \tag{A. 1}$$

where the N_n are the eigenvalues of the integral equation

$$\int_0^T R(x-y)\, \phi_i(y)\, dy = N_i \phi_i(x), \qquad 0 \leq x \leq T.$$

$R(\tau)$ is the noise autocorrelation function, and $N(w)$ is its Fourier transform. $G(\cdot)$ is any bounded nonincreasing function such that the right side of (A. 1) exists.

Proof: We start with a theorem of Kac, Murdock, and Szego[12] (also see Grenander and Szego[10]) that if $R(\tau)$ and $N(w)$ are absolutely integrable on $-\infty, \infty$, and $R(\tau)$ continuous, then

$$\lim_{T\to\infty} \frac{N_T(a, b)}{T} = \sigma(w, a < N(w) < b)/2\pi, \tag{A. 2}$$

where $N_T(a, b)$ is the number of eigenvalues between a and b, and $\sigma(w; a<N(w)<b)$ is the measure of the set of w for which $N(w)$ is between a and b, as long as the interval $[a, b]$ does not include zero, and the set of w for which $N(w) = a$ and $N(w) = b$ is of measure zero.

The restriction that $R(\tau)$ is integrable can be avoided by the argument used in Section II. We can have

$$R(\tau) = N_o \mu_o(\tau) - R'(\tau)$$

with $R'(\tau)$ integrable. The only change in the theorem is that the interval $[a, b]$ must not include N_o.

We rewrite equation (A. 2) as

$$\lim_{T\to\infty} \frac{N_T(a, b)}{T} = \frac{1}{2\pi} \int_{-\infty}^{\infty} X_{a,b}[N(w)]\, dw,$$

where

$$X_{a,b}[N(w)] = \begin{cases} 1; & a < N(w) < b \\ 0; & \text{otherwise} \end{cases}$$

Now break up the domain of $G(\cdot)$ into an arbitrary set of intervals divided by the points

$$a_o < a_1 < \ldots < a_I.$$

Then if G is monotone decreasing, we can write

$$\frac{1}{2\pi} \sum_{i=1}^{I} \int_{-\infty}^{\infty} G(a_i)\, X_{a_{i-1}, a_i} [N(w)]\, dw \leq \sum_{i=1}^{I} \lim_{T\to\infty} \frac{\sum_{j=1}^{N_T(a_{i-1}, a_i)} G(N_{i,j})}{T}$$

$$\leq \frac{1}{2\pi} \sum_{i=1}^{I} \int_{-\infty}^{\infty} G(a_{i-1})\, X_{a_{i-1}, a_i} [N(w)]\, dw. \tag{A.3}$$

This is seen to be true, since for any i

$$G(a_i) \leq G(N_j) \leq G(a_{i-1}),$$

where N_j is any N_i between a_i and a_{i-1}. Since I is finite, the sum and the integral can be interchanged in the outer terms of (A.3), and the sum can be taken inside the limit in the inner term.

$$\frac{1}{2\pi} \int_{-\infty}^{\infty} \sum_{i=1}^{I} G(a_i)\, X_{a_{i-1}, a_i} [N(w)]\, dw \leq \lim_{T\to\infty} \frac{\sum_{j=1}^{N_T(a_o, a_I)} G(N_{i,j})}{T}$$

$$\leq \frac{1}{2\pi} \int_{-\infty}^{\infty} \sum_{i=1}^{I} G(a_{i-1})\, X_{a_{i-1}, a_i} [N(w)]\, dw. \tag{A.4}$$

The limit of the center term is independent of the subdivision, as long as $[a_o, a_I]$ does not include N_o, but does cover the entire range of $G[N(w)]$ when w goes from $-\infty$ to ∞.

The expressions on the right and left are the integrals of simple functions. The simple function on the left is less than $G[N(w)]$, and the simple function on the right is greater. Also, any simple function will generate a finite set of a_i which can be used to generate the right and left integrals. If $G[N(w)]$ is bounded above and below and

$$\int_{-\infty}^{\infty} G[N(w)]\, dw \tag{A.5}$$

exists, then by definition there is a monotone increasing sequence of simple functions converging to $G[N(w)]$ from below almost everywhere, whose integral converges to (A.5), and likewise for a sequence converging from above. Thus, given $\epsilon > 0$, there exists a finite set of a_i such that the left and right side of (A.4) differ by less than ϵ. To extend this to monotone nonincreasing $G(\cdot)$, we need only assure ourselves that the a_i can always be chosen so that the measure of the sets $N(w) = a_i$ is zero. This excludes only a finite number of values taken on by $G(\cdot)$ and there is no difficulty in avoiding those values. This proves the theorem.

APPENDIX B

Asymptotic Behavior of q

We have a sum of independent random variables each of which is the square of a Gaussianly distributed variable with zero mean and variance Q_n. Consequently, the sum has mean

$$\sum_n Q_n = S$$

and variance

$$2 \sum_n Q_n^2.$$

We wish to find a lower bound on the probability that the sum lies between S and S - δ.

The central limit theorem states that given a sequence of independent random variables Z_i, $1 \leq i \leq n$, with means $\bar{Z}_i$, variances σ_i^2, and third absolute moments

$$\beta_{3,i} = \overline{|Z_i - \bar{Z}_i|^3} < \infty,$$

and if G(x) is the distribution function of the normalized sum, then

$$|G(x) - \Phi(x)| \leq \frac{C\rho_{3,n}}{\sqrt{n}},$$

where $\Phi(x)$ is the normal distribution function,

$$\beta_{3,n} = \frac{\frac{1}{n} \sum_{i=1}^{n} \beta_{3,i}}{\left[\frac{1}{n} \sum_{i=1}^{n} \sigma_i^2\right]^{3/2}},$$

and C is a constant less than 7.5. For our particular problem

$$\beta_{3,i} \leq \frac{17}{2} Q_i^3.$$

Thus we write

$$\frac{C\rho_{3,n}}{\sqrt{n}} = \frac{17C \sum_{i=1}^{n} Q_i^3}{4\sqrt{2}\left(\sum_{i=1}^{n} Q_i^2\right)^{3/2}}.$$

We underbound

$$q = G(0) - G\left(-\frac{\delta}{\sqrt{2\sum_{i=1}^{n} Q_i^2}}\right)$$

by

$$\Phi(0) - \Phi\left(-\frac{\delta}{\sqrt{2\sum_{i=1}^{n} Q_i^2}}\right) - \frac{2C\rho_{3,n}}{\sqrt{n}}.$$

We note that $\sum_{i=1}^{n} Q_i^2$ grows linearly with T. Therefore, since $\Phi'(0) = \frac{1}{\sqrt{2\pi}}$, we have for large enough T

$$q \geqslant \frac{\delta}{4\sqrt{\pi \sum_{i=1}^{n} Q_i^2}} - \frac{17C \sum_{i=1}^{n} Q_i^3}{4\sqrt{2}\left(\sum_{i=1}^{n} Q_i^2\right)^{3/2}} = \frac{\sqrt{2}\sum_{i=1}^{n} Q_i^2 - 17C\sqrt{\pi}\sum_{i=1}^{n} q_i^3}{4\sqrt{2\pi\left(\sum_{i=1}^{n} Q_i^2\right)^3}}$$

We now use the fact, proved in Appendix A, that the sums approach a constant times T for a solution with Q_i defined in terms of N_i, N_b, and ρ. Let

$$\sum_{i=1}^{n} Q_i^2 \xrightarrow[T\to\infty]{} TD_2,$$

$$\sum_{i=1}^{n} Q_i^3 \xrightarrow[T\to\infty]{} TD_3,$$

then for large enough T

$$q \geqslant \frac{\sqrt{2}\ \delta D_2 - 17C\sqrt{\pi}\ D_3}{4\sqrt{2\pi D_2 T}}.$$

If we let

$$\delta = \frac{4\sqrt{2\pi D_2} + 17C\sqrt{\pi}\ D_3\sqrt{2}\ D_2}{\sqrt{2}\ D_2},$$

then $q \geqslant \frac{1}{\sqrt{T}}$, and $\frac{1}{q} \leqslant \sqrt{T}$.

APPENDIX C

Proof of Upper Bound on P_e for List Decoding

This proof closely follows Gallager's[8] proof for a single guess at the output. The first result was first obtained by Gallager, and is similar to that obtained by Elias[4] for the binary symmetric channel.

We start with the standard expression for P_{em} in the integral form for a channel with continuous input and output and a given set of code words $\underline{x}_i$

$$P_{em} = \int_{\underline{y}} P(\underline{y}/\underline{x}_m)\, \phi_m(\underline{y})\, d\underline{y}, \tag{C. 1}$$

where

$$\phi_m(\underline{y}) = \begin{cases} 1; & \text{if } P(\underline{y}/\underline{x}_m) \le P\left(\underline{y}/\underline{x}_{m_i}\right) \text{ for at least } L \text{ distinct } m_i \ne m \\ 0; & \text{otherwise} \end{cases}$$

The inequality

$$\phi_m(\underline{y}) \le$$

$$\left(\frac{\displaystyle\sum_{m_1 \ne m} \sum_{m_2 \ne m, m_1} \cdots \sum_{m_L \ne m, \ldots, m_{L-1}} \left[P\left(\underline{y}/\underline{x}_{m_1}\right) P\left(\underline{y}/\underline{x}_{m_2}\right) \cdots P\left(\underline{y}/\underline{x}_{m_L}\right) \right]^{1/(1+\rho)}}{P(\underline{y}/\underline{x}_m)^{L/(1+\rho)}\, L!} \right)^{\rho/L}$$

follows, since in the numerator sum there are at least L! ways to have all the P be those that are larger than $P(\underline{y}/\underline{x}_m)$. Taking the inside terms to the $1/(1+\rho)$ power, and the result to the ρ/L power does not affect the inequality.

We can bound (C. 1) and take the average over an ensemble of codes in which, for each m, $\underline{x}_m$ is chosen with the probability assignment $P(\underline{x})$.

$$\overline{P}_e \le \overline{\int_{\underline{y}} P(\underline{y}/\underline{x}_m)^{1/(1+\rho)} \left(\sum_{m_1 \ne m} \cdots \sum_{m_L \ne m, m_1, \ldots, m_{L-1}} \left[P\left(\underline{y}/\underline{x}_{m_1}\right) \cdots P\left(\underline{y}/\underline{x}_{m_L}\right) \right]^{1/(1+\rho)} \frac{1}{L!} \right)^{\rho/L} d\underline{y}}. \tag{C. 2}$$

Since the $\underline{x}_i$ are selected independently over the ensemble of codes $P(\underline{y}/\underline{x}_m)$ and all the $P\left(\underline{y}/\underline{x}_{m_i}\right)$ are independent random variables for any given $\underline{y}$, and for any random variable $\overline{\xi^{\rho/L}} \leq \bar{\xi}^{\rho/L}$ when $\rho/L \leq 1$, we can write (C.2) with the average bar only over the $P\left(\underline{y}/\underline{x}_{m_i}\right)^{1/(1+\rho)}$ terms. Since all these averages are the same we can write

$$\overline{P}_e \leq \int_{\underline{y}} \left(\frac{(M-1)!}{(M-1-L)!\,L!}\right)^{\rho/L} \left(\int_{\underline{x}} P(\underline{x})\, P(\underline{y}/\underline{x})^{1/(1+\rho)}\, d\underline{x}\right)^{1+\rho} d\underline{y}, \qquad \rho \leq L.$$

We observe that by Stirling's formula

$$\ln \frac{(M-1)!}{(M-1-L)!\,L!} \leq L \ln \frac{Me}{L}.$$

Thus we can write

$$\overline{P}_e \leq \exp -[E_o(\rho)-\rho R],$$

where

$$E_o(\rho) = -\ln \int_{\underline{y}} \left(\int_{\underline{x}} P(\underline{x})\, P(\underline{y}/\underline{x})^{1/(1+\rho)}\right)^{1+\rho} d\underline{y},$$

and $R = \ln \frac{Me}{L}$.

We derive the expurgated bound by setting $\rho = L$ in the expression for P_{em} for any particular code. (This is identical to (C.2) but without the average bar.) Then we define

$$Q\left(\underline{x}_m, \underline{x}_{m_1}, \dots \underline{x}_{m_L}\right) = \int_{\underline{y}} \left[P(\underline{y}/\underline{x}_m)\, P\left(\underline{y}/\underline{x}_{m_1}\right) \cdots P\left(\underline{y}/\underline{x}_{m_L}\right)\right]^{1/(1+L)} d\underline{y},$$

which is a random variable over the ensemble of codes. Also, both sides of the inequality

$$P_{em} \leq \frac{1}{L!} \sum_{m_1 \neq m} \cdots \sum_{m_L \neq m, \dots m_{L-1}} Q\left(\underline{x}_m, \underline{x}_{m_1} \cdots \underline{x}_{m_L}\right)$$

are random variables over the ensemble of random codes. Now for a given number B, to be determined later, define the random variable

$$\gamma_m(\text{code}) = \begin{cases} 1; & \text{if } P_{em} \geq B \\ 0; & \text{otherwise} \end{cases}$$

The inequality

$$\gamma_m(\text{code}) \leq \sum_{m_1 \neq m} \cdots \sum_{m_L \neq m, \dots m_{L-1}} \frac{Q\left(\underline{x}_m, \cdots \underline{x}_{m_L}\right)^s}{(BL!)^s}; \qquad 0 \leq s \leq 1$$

follows, in that it is true for s = 1 and decreasing s makes the individual terms in the sum that are less than 1 larger, and if any term is larger than 1 it is true anyway.

We wish to purge from our ensemble less than 1/2 of code words, and we will do this by deleting all code words for which the random variable P_{em} is greater than B, and we shall choose B so that over the ensemble less than 1/2 of the code words will be purged.

$$P(P_{em} \geq B) = \overline{\gamma_n(\text{code})}$$

This is the probability that a given code word will be expurgated. If we make this probability equal or less than 1/2, then there exists a code with at least M/2 code words satisfying $P_{em} \leq B$.

$$\overline{\gamma_m(\text{code})} \leq \overline{\sum_{m_1 \neq m} \cdots \sum_{m_L \neq m, \ldots m_{L-1}} \frac{Q\left(\underline{x}_m, \ldots \underline{x}_{m_L}\right)^s}{(BL!)^s}} = \frac{1}{2}.$$

Then we solve for B, take the average inside the sum, and note that the average does not depend on which m_i are used, just that they be different. Also, for this reduced set of code words, $P_e \leq B$; thus

$$P_e \leq B = \left[2 \frac{(M-1)!}{(M-1-L)!\,(L!)^s} \overline{\left(\int_{\underline{y}} P(\underline{y}/\underline{x}_m)^{1/(1+L)} \cdots P\left(\underline{y}/\underline{x}_{m_L}\right)^{1/(1+L)} d\underline{y}\right)^s}\right]^{1/s}$$

$$\text{all } m_i \text{ different} \qquad \text{(C.3)}$$

Let $s = \frac{L}{\rho}$, $\rho \geq L$, then we can write (C. 3)

$$P_e \leq \exp -[E_o(\rho) - \rho R],$$

where

$$E_o(\rho) = -\frac{\rho}{L} \ln \int_{\underline{x}_m} \cdots \int_{\underline{x}_{m_L}} P(\underline{x}_m) \cdots P\left(\underline{x}_{m_L}\right)$$

$$\cdot \left(\int_{\underline{y}} \left[P(\underline{y}/\underline{x}_m) \cdots P\left(\underline{y}/\underline{x}_{m_L}\right)\right]^{1/(1+L)}\right)^{L/\rho}, \qquad \rho \geq L$$

and

$$R = \ln 4eM - \frac{L}{\rho} \ln L.$$

Here, we have taken into account the fact that 1/2 of the original code words have been deleted.

APPENDIX D

Proof of Two Theorems on the Lower Bound to P_e for Optimum Codes

This entire appendix is a copy of two theorems and their proofs given by R. G. Gallager[21] in an unpublished paper. They are presented here because of their general unavailability and because the theorems are essential to the results of this report.

The first theorem corresponds to that given in Section III by making the following correspondences:

Section II		Appendix D
$P(\underline{y}/\underline{x}_m)$	. . . .	$P_1(\underline{y})$
$f(\underline{y})$	. . . .	$P_2(\underline{y})$
P_{em}	. . . .	P_{e1}
Z_m	. . . .	P_{e2}

Theorem 3

Let $\underline{y} = (j_1, j_2, \ldots, j_N)$, $1 \leq j_n \leq J$, $1 \leq n \leq N$, represent an arbitrary sequence of N integers, 1 to J, and let

$$P_1(\underline{y}) = \prod_{n=1}^{N} P_{1n}(j_n); \quad P_2(\underline{y}) = \prod_{n=1}^{N} P_{2n}(j_n) \tag{2.1}$$

be two product probability measures on the sequences $\underline{y}$. Let Y_1 be an arbitrary set of sequences $\underline{y}$ and let Y_1^c be its complement. Let

$$P_{e1} = \sum_{\underline{y} \in Y_1^c} P_1(\underline{y}); \quad P_{e2} = \sum_{\underline{y} \in Y_1} P_2(\underline{y}). \tag{2.2}$$

Let s be an arbitrary number, $0 < s < 1$, and define

$$\mu_n(s) = \ln \sum_{j_n=1}^{J} P_{1n}^{1-s}(j_n)\, P_{2n}^{s}(j_n); \quad 1 \leq n \leq N. \tag{2.3}$$

Assume that for each n, $\mu_n(s)$ is finite (this corresponds to assuming that $P_1(\underline{y})\, P_2(\underline{y}) \neq 0$ for some $\underline{y}$). Then if

$$P_{e2} \leq \frac{1}{4} \exp\left(\sum_{n=1}^{N} [\mu_n(s) + (1-s)\mu_n'(s)] - (1-s) \sqrt{2 \sum_{n=1}^{N} \mu_n''(s)} \right), \tag{2.4}$$

it must follow that

$$P_{e1} \geq \frac{1}{4} \exp\left(\sum_{n=1}^{N} [\mu_n(s) - s\mu_n'(s)] - s \sqrt{2 \sum_{n}^{N} \mu_n''(s)} \right), \tag{2.5}$$

where $\mu_n'(s)$ and $\mu_n''(s)$ are the derivatives of $\mu_n(s)$ with respect to s.

Proof of Theorem 3

Define

$$\mu(s) = \sum_{n=1}^{N} \mu_n(s) = \ln \prod_{n=1}^{N} \sum_{j_n=1}^{J} P_{1n}^{1-s}(j_n)\, P_{2n}^{s}(j_n) \tag{2.8}$$

$$= \ln \sum_{\underline{y}} P_1^{1-s}(\underline{y})\, P_2^{s}(\underline{y}), \tag{2.9}$$

where we have used Eq. 2.1 to go from Eq. 2.8 to 2.9. The sum over $\underline{y}$ in Eq. 2.9 can be considered to be either over all output sequences $\underline{y}$ or over all sequences in the overlap region where both $P_1(\underline{y})$ and $P_2(\underline{y})$ are nonzero. For the rest of the proof, we shall consider all sums over $\underline{y}$ to be only over the overlap region.

Taking the derivations of $\mu(s)$, we get

$$\mu'(s) = \sum_{\underline{y}} \frac{P_1^{1-s}(\underline{y})\, P_2^{s}(\underline{y})}{\sum_{\underline{y}'} P_1^{1-s}(\underline{y}')\, P_2^{s}(\underline{y}')} \ln \frac{P_2(\underline{y})}{P_1(\underline{y})} \tag{2.10}$$

$$\mu''(s) = \sum_{\underline{y}} \frac{P_1^{1-s}(\underline{y})\, P_2^{s}(\underline{y})}{\sum_{\underline{y}'} P_1^{1-s}(\underline{y}')\, P_2^{s}(\underline{y}')} \ln \left(\frac{P_2(\underline{y})}{P_1(\underline{y})}\right)^2 - [\mu'(s)]. \tag{2.11}$$

For a given s, $0 < s < 1$, define

$$q_s(\underline{y}) = \frac{P_1^{1-s}(\underline{y})\, P_2^{s}(\underline{y})}{\sum_{\underline{y}'} P_1^{1-s}(\underline{y}')\, P_2^{s}(\underline{y}')} \tag{2.12}$$

$$D(\underline{y}) = \ln \frac{P_2(\underline{y})}{P_1(\underline{y})}. \tag{2.13}$$

If we consider $D(\underline{y})$ to be a random variable with probability measure $q_s(\underline{y})$, then we see from Eqs. 2.10 and 2.11 that $\mu'(s)$ and $\mu''(s)$ are the mean and variance of $D(\underline{y})$, respectively. Now let Y_s be the set of sequences $\underline{y}$ for which $D(\underline{y})$ is within $\sqrt{2}$ standard deviations of its mean.

$$Y_s = [\underline{y} : |D(\underline{y}) - \mu'(s)| \leqslant \sqrt{2\mu''(s)}\,]. \tag{2.14}$$

From the Chebyshev inequality,

$$\sum_{\underline{y} \in Y_s} q_s(\underline{y}) \geqslant \frac{1}{2}. \tag{2.15}$$

We can now use Eq. 2.12 to relate $P_1(\underline{y})$ to $q_s(\underline{y})$ for those $\underline{y}$ in the overlap region.

$$P_1(\underline{y}) = \left(\sum_{\underline{y}'} P_1^{1-s}(\underline{y}')\, P_2^s(\underline{y}')\right)\left(\frac{P_1(\underline{y})}{P_2(\underline{y})}\right)^s q_s(\underline{y}).$$

Using Eqs. 2.13 and 2.9, this yields

$$P_{e1} \geqslant \sum_{\underline{y} \in Y_1^c} P_1(\underline{y}) = e^{\mu(s)} \sum_{\underline{y} \in Y_1^c} e^{-sD(\underline{y})}\, q_s(\underline{y}). \tag{2.16}$$

The inequality in Eq. 2.16 comes from the fact that we are now interpreting sums over y to be only over the overlap region where both $P_1(\underline{y})$ and $P_2(\underline{y})$ are nonzero, whereas in Eq. 2.9, the sum is over all $\underline{y} \in Y_1^c$. For any reasonable decision scheme, of course, Y_1^c would not include any $\underline{y}$ for which $P_1(\underline{y}) \neq 0$ and $P_2(\underline{y}) = 0$, and in this case Eq. 2.16 is true with equality. Treating $P_2(\underline{y})$ in the same way as $P_1(\underline{y})$, we get

$$P_{e2} \geqslant \sum_{\underline{y} \in Y_1} P_2(\underline{y}) = e^{\mu(s)} \sum_{\underline{y} \in Y_1} e^{(1-s)D(\underline{y})}\, q_s(\underline{y}). \tag{2.17}$$

Now we can lower-bound P_{e1} by summing over only those $\underline{y}$ in both Y_1^c and Y_s, to obtain

$$P_{e1} \geqslant e^{\mu(s)} \sum_{\underline{y} \in Y_1^c Y_s} e^{-sD(\underline{y})}\, q_s(\underline{y}) \tag{2.18}$$

$$\geqslant \exp[\mu(s) - s\mu'(s) - s2\mu''(s)] \sum_{\underline{y} \in Y_1^c Y_s} q_s(\underline{y}). \tag{2.19}$$

In Eq. 2.19, we have used Eq. 2.14 to upper-bound $D(\underline{y})$, thereby lower-bounding $e^{-sD(\underline{y})}$. Using the same procedure to lower-bound P_{e2}, we get

$$P_{e2} \geqslant \exp[\mu(s) - (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}\,] \sum_{\underline{y} \in Y_1 Y_s} q_s(\underline{y}). \tag{2.20}$$

Comparing Eq. 2.20 with the hypothesis, Eq. 2.4, and using Eq. 2.8, we see that

$$\sum_{\underline{y} \in Y_1 Y_s} q_s(\underline{y}) \leq \frac{1}{4}. \tag{2.21}$$

Combining Eq. 2.21 with 2.15, we get

$$\sum_{\underline{y} \in Y_1^c Y_s} q_s(\underline{y}) \geq \frac{1}{4}. \tag{2.22}$$

Finally substituting Eq. 2.22 in Eq. 2.19, we get Eq. 2.5, thereby proving the theorem.

Theorem 5

Let $P_1(N_1, M, L)$ be a lower bound on the average probability of list decoding error for any code of block length N_1 with M code words and decoding list of size L on a particular discrete memoryless channel when the code words are used with an arbitrary set of probabilities $p(m)$. Let $P_2\left(N_2, \frac{L}{2}\right)$ be a lower bound to probability of decoding error for at least one word in any code of block length N_2 with $\frac{L}{2}$ code words for the same channel. Then any code of blocklength $N = N_1 + N_2$ with M code words, used with probabilities $p(m)$ has an average probability of decoding error bounded by

$$P_e \geq \frac{P_1(N_1, M, L)\, P_2(N_2, L/2)}{4}. \tag{4.2}$$

Proof:

Let $\underline{x}_1, \dots, \underline{x}_M$ be the code words for any given code of block length N. Let $\underline{y}$ be a received sequence and let $\underline{y}_1$ be the first N_1 letters of $\underline{y}$, and let $\underline{y}_2$ be the final N_2 letters of $\underline{y}$. The probability that m will be transmitted and $\underline{y}_1\underline{y}_2$ received is, then,

$$P(m, \underline{y}_1, \underline{y}_2) = p(m)\, \Pr(\underline{y}|\underline{x}_m) = p(m)\, \Pr(\underline{y}_1|\underline{x}_m)\, \Pr(\underline{y}_2|\underline{x}_m), \tag{4.3}$$

where in the second equality we have used the fact that the channel is memoryless.

For any given received sequence $\underline{y}$, the decoder minimizes the probability of error by decoding that sequence m that maximizes $\Pr(m|\underline{y})$, or equivalently that maximizes $P(m, \underline{y}_1, \underline{y}_2)$. Let Y_m be the set of $\underline{y}$ for which $\Pr(m|\underline{y}) > \Pr(m'|\underline{y})$ for all $m' \neq m$. Note that it is possible for $\Pr(m|\underline{y})$ to be maximized by several different values of m. In this case the decoder can do no better than to choose at random between those m that maximize $\Pr(m|\underline{y})$, thus making an error with probability at least 1/2 and at most 1. Thus for a given code, decoding for minimum error probability, we have

$$\overline{P}_e \geq \frac{1}{2} \sum_{m=1}^{M} \sum_{\underline{y} \in Y_m^c} P(m, \underline{y}_1, \underline{y}_2) \tag{4.4}$$

$$\overline{P}_e \leqslant \sum_{m=1}^{M} \sum_{\underline{y} \in Y_m^c} P(m)\, P(\underline{y}|\underline{x}_m). \tag{4.5}$$

We can break up Eq. 4.4 in the following way, using Eq. 4.3 and Bayes' rule.

$$P_e \geqslant \frac{1}{2} \sum_{\underline{y}_1} P(\underline{y}_1) \left(\sum_{m, \underline{y}_2 : \underline{y} \in Y_m^c} P(m|\underline{y}_1)\, P(\underline{y}_2|\underline{x}_m) \right). \tag{4.6}$$

Define the term in braces as $P_e(\underline{y}_1)$,

$$P_e(\underline{y}_1) = \sum_{m, \underline{y}_2 : \underline{y} \in Y_m^c} P(m|\underline{y}_1)\, P(\underline{y}_2|\underline{x}_m). \tag{4.7}$$

For notational convenience, we now consider renumbering the messages for a particular sequence $\underline{y}$, in decreasing order of a posteriori probability

$$P(m=1|\underline{y}_1) \geqslant P(m=2|\underline{y}_1) \geqslant \dots \geqslant P(m=M|\underline{y}_1). \tag{4.8}$$

Since the sum over m in Eq. 4.7 is over all m, clearly Eq. 4.7 is still valid after this

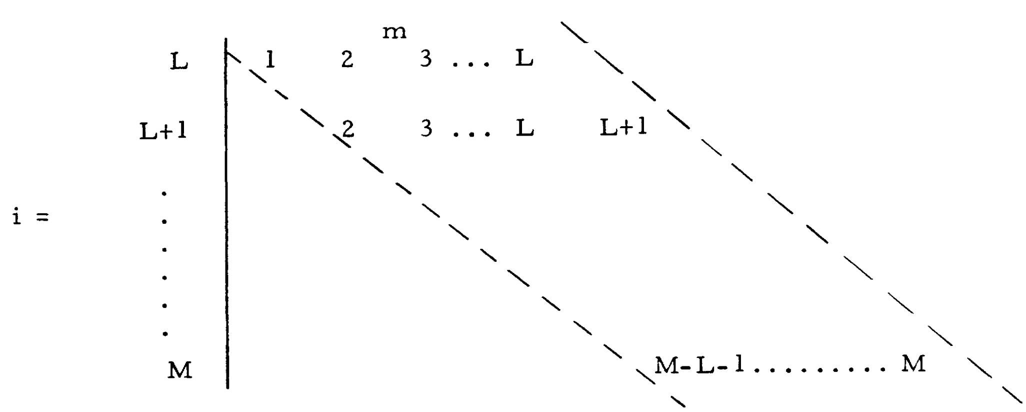


Fig. 4.1.

renumbering. Now we split the sum over m into 2 terms in such a way that each term is counted at most L times (see Fig. 4.1).

$$P_e(\underline{y}_1) \geqslant \frac{1}{L} \sum_{i=L}^{M} \sum_{m=i-L+1}^{i} \sum_{\underline{y}_2 : \underline{y} \in Y_m^c} P(m|\underline{y}_1)\, P(\underline{y}_2|\underline{x}_m). \tag{4.9}$$

Equation 4.9 can now be further lower-bounded by summing only over those $\underline{y}_2$ for which

$$P(m|\underline{y}_1)\, P(\underline{y}_2|\underline{x}_m) \leq P(m'|\underline{y}_1)\, P(\underline{y}_2|\underline{x}_{m'}) \tag{4.10}$$

$$\text{some } m',\ i-L+1 \leq m' \leq i.$$

If Eq. 4.10 is satisfied for a given $\underline{y}_1$, $\underline{y}_2$, and i, then $\underline{y}$ is certainly in Y_m^c.

$$P_e(\underline{y}_1) \geq \frac{1}{L} \sum_{i=L}^{M} \sum_{m=i-L+1}^{i} \sum_{\underline{y}_2:\text{Eq. 4.10 valid}} P(m|\underline{y}_1)\, P(\underline{y}_2|\underline{x}_m) \tag{4.11}$$

Now define, for $i-L+1 \leq m \leq i$,

$$q_{\underline{y}_1,i}(m) = \frac{P(m|\underline{y}_1)}{\sum\limits_{m'=i-L+1}^{i} P(m'|\underline{y}_1)} \tag{4.12}$$

$$P_e(\underline{y}_1) \geq \frac{1}{L} \sum_{i=L}^{M} \left(\sum_{m'=i-L+1}^{i} P(m'|\underline{y}_1) \right) \left(\sum_{m=i-L+1}^{i} \sum_{\underline{y}_2:\text{Eq. 4.10 valid}} q_{\underline{y}_1,i}(m)\, P(\underline{y}_2|\underline{x}_m) \right). \tag{4.13}$$

The term in braces in Eq. 4.13 is in the same form as Eq. 4.5. It is an upper bound to the probability of decoding error for a code of block length N_2 with L code words with a priori probabilities $q_{\underline{y}_1,i}(m)$ for $i-L+1 \leq m \leq i$. We can think of the code words here as being the last N_2 letters of each of the original code words $\underline{x}_m$. By applying Lemma 1 (Eq. 3.37), the probability of error for such a code is lower-bounded by

$$\frac{L}{2} P_2\left(N_2, \frac{L}{2}\right) \min_{i-L+1 \leq m \leq i} q_{\underline{y}_1,i}(m). \tag{4.14}$$

Because of the ordering of the m, the minimum above occurs for m=i. Also, since the quantity in braces in Eq. 4.13 is an upper bound to the error probability for which Eq. 4.14 is a lower bound, we have

$$P_e(\underline{y}_1) \geq \frac{1}{L} \sum_{i=L}^{M} \left(\sum_{m=i-L+1}^{i} P(m|\underline{y}_1) \right) \frac{L}{2} P_2\left(N_2, \frac{L}{2}\right) q_{\underline{y}_1,i}(i) \tag{4.15}$$

$$P_e(\underline{y}_1) \geq \frac{1}{2} \sum_{i=L}^{M} P_2\left(N_2, \frac{L}{2}\right) P(i|\underline{y}_1), \tag{4.16}$$

where we have used Eq. 4.12.

Substituting Eq. 4.16 back in Eq. 4.6, we have

$$P_e \geq \frac{1}{4} \left(\sum_{\underline{y}_1} P(\underline{y}_1) \sum_{i=L}^{M} P(i|\underline{y}_i) \right) P_2\left(N_2, \frac{L}{2}\right). \tag{4.17}$$

Further reducing Eq. 4.17 by summing from $i=L+1$ to M, we see that the term in brackets is the probability of list decoding for a code of block length N_1, with M code words and a list of size L. This completes the proof of the theorem.

Acknowledgment

I am greatly indebted to Professor Robert G. Gallager for his guidance during my thesis research and for the theoretical foundations for this report. He has helped me avoid numerous mistakes and has pointed out ways to shorten several of the proofs.

Thanks are due to Professor John M. Wozencraft who acted as a reader and made several timely suggestions about which problem to pursue.

Professor Robert S. Kennedy, who also acted as a reader, and many other members of the faculty and graduate students in the Processing and Transmission of Information Group of the Research Laboratory of Electronics, M.I.T., have contributed to this work through discussions and by pointing out possible errors.

I am grateful to the Research Laboratory of Electronics and its sponsors and to a National Science Foundation Fellowship for support during the period of my graduate studies.

References

1. E. R. Berlekamp, "Block Coding with Noiseless Feedback," Ph.D. Thesis, Department of Electrical Engineering, Massachusetts Institute of Technology, 1964.
2. W. B. Davenport and W. L. Root, An Introduction to the Theory of Random Signals and Noise (McGraw-Hill Book Company, New York, 1958).
3. P. M. Ebert, "Error Bounds for Gaussian Noise Channels," Quarterly Progress Report No. 77, Research Laboratory of Electronics, M.I.T., Cambridge, Mass., April 15, 1965, pp. 292-302.
4. P. Elias, "List Decoding for Noisy Channels," Technical Report 335, Research Laboratory of Electronics, M.I.T., Cambridge, Mass., September 20, 1957.
5. R. M. Fano, Transmission of Information (The M.I.T. Press, Cambridge, Mass., and John Wiley and Sons, Inc., New York, 1961).
6. A. Feinstein, "Error Bounds in Noisy Channels without Memory," IRE Trans., Vol. IT-1, pp. 13-14, 1955.
7. G. D. Forney, "Concatenated Codes," Technical Report 440, Research Laboratory of Electronics, M.I.T., Cambridge, Mass., December 1, 1965.
8. R.G. Gallager, "A Simple Derivation of the Coding Theorem and Some Applications," IEEE Trans., Vol. IT-11, pp. 3-18, 1965.
9. R. G. Gallager, "Lower Bounds on the Tails of Probability Distributions," Quarterly Progress Report No. 77, Research Laboratory of Electronics, M.I.T., Cambridge, Mass., April 15, 1965, pp. 277-291.
10. U. Grenander and G. Szego, Toeplitz Forms and Their Applications (University of California Press, Berkeley, 1958).
11. J. L. Holsinger, "Digital Communication over Fixed Time-Continuous Channels with Memory – With Special Application to Telephone Channels," Ph.D. Thesis, Department of Electrical Engineering, Massachusetts Institute of Technology, 1964.
12. M. Kac, W. L. Murdock, and G. Szego, "On the Eigenvalues on Certain Hermitian Forms," J. Rational Mech. Analysis 2, 767-800 (1953); cf. Theorem 2.
13. J. L. Kelly, "A Class of Codes for Signaling on a Noisy Continuous Channel," IRE Trans., Vol. IT-6, p. 22, 1960.
14. H. W. Kuhn and A. W. Tucker, "Non-linear Programming," Proceedings of the Second Berkeley Symposium on Mathematical Statistics and Probability, 1951, pp. 481-492.
15. W. W. Peterson, Error Correcting Codes (The M.I.T. Press, Cambridge, Mass., and John Wiley and Sons, Inc., New York, 1961).
16. S. O. Rice, "Communication in the Presence of Noise – Probability of Error of Two Encoding Schemes," Bell System Tech. J. 29, 60 (1950).
17. C. E. Shannon, "A Mathematical Theory of Communication," Bell System Tech. J. 27, pp. 379, 623 (1949).
18. C. E. Shannon, "Communication in the Presence of Noise," Proc. IRE 37, 1 (1949).
19. C. E. Shannon, "Certain Results in Coding Theory for Noisy Channels," Inform. Contr. 1, 6-25 (1957).
20. C. E. Shannon, "Probability of Error for Optical Codes in a Gaussian Channel," Bell System Tech. J. 38, 611-652 (1957).
21. C. E. Shannon, R. G. Gallager, and E. R. Berlekamp, "Lower Bounds to Error Probability for Coding Discrete Memoryless Channels" (to appear in Information and Control).
22. C. E. Shannon, "Coding Theorems for Discrete Source with a Fidelity Criterion," IRE National Convention Record, Part 4, pp. 142-163, 1959.

23. J. Wolfowitz, Coding Theorem of Information Theory (Prentice Hall, New York, 1961); or see "Strong Converse of the Theorem for General Discrete Finite Memory Channels," Inform. Contr. 3, 89-93 (1960).

24. J. M. Wozencraft and B. Reiffen, Sequential Decoding (The Technology Press of Massachusetts Institute of Technology, Cambridge, Mass., and John Wiley and Sons, Inc., New York, 1961).

25. J. M. Wozencraft et al., "Seco: A Self-regulating Error Correcting Coder-Decoder," IRE Trans., Vol. IT-8, pp. s124-135, 1962; also see "Applications of Sequential Decoding to High-Rate Data Communication on a Telephone Line," IEEE Trans., Vol. IT-9, pp. 124-126, 1963.

26. A. D. Wyner, "An Improved Bound for Gaussian Channels," Bell System Tech. J. 43, 3070 (1964).

27. J. Ziv, "Coding and Decoding for Time-Discrete Amplitude-Continuous Memoryless Channels," IRE Trans., Vol. IT-8, pp. s199-s205, 1962.

JOINT SERVICES ELECTRONICS PROGRAM
REPORTS DISTRIBUTION LIST

Department of Defense

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

Office of Deputy Director
(Research and Information Room 3D1037)
Department of Defense
The Pentagon
Washington, D.C. 20301

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

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

Headquarters
Defense Communications Agency (333)
The Pentagon
Washington, D.C. 20305

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

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

Weapons Systems Evaluation Group
Attn: Col. Finis G. Johnson
Department of Defense
Washington, D.C. 20305

National Security Agency
Attn: R4-James Tippet
Office of Research
Fort George G. Meade, Maryland 20755

Central Intelligence Agency
Attn: OCR/DD Publications
Washington, D.C. 20505

Department of the Air Force

AUL3T-9663
Maxwell AFB, Alabama 36112

AFRSTE
Hqs. USAF
Room ID-429, The Pentagon
Washington, D.C. 20330

AFFTC (FTBPP-2)
Technical Library
Edwards AFB, Calif. 93523

Space Systems Division
Air Force Systems Command
Los Angeles Air Force Station
Los Angeles, California 90045
Attn: SSSD

SSD(SSTRT/Lt. Starbuck)
AFUPO
Los Angeles, California 90045

Det #6, OAR (LOOAR)
Air Force Unit Post Office
Los Angeles, California 90045

Systems Engineering Group (RTD)
Technical Information Reference Branch
Attn: SEPIR
Directorate of Engineering Standards
and Technical Information
Wright-Patterson AFB, Ohio 45433

ARL (ARIY)
Wright-Patterson AFB, Ohio 45433

AFAL (AVT)
Wright-Patterson AFB, Ohio 45433

AFAL (AVTE/R. D. Larson)
Wright-Patterson AFB, Ohio 45433

Commanding General
Attn: STEWS-WS-VT
White Sands Missile Range
New Mexico 88002

RADC (EMLAL-1)
Griffiss AFB, New York 13442
Attn: Documents Library

AFCRL (CRMXLR)
AFCRL Research Library, Stop 29
L. G. Hanscom Field
Bedford, Massachusetts 01731

Academy Library DFSLB)
U.S. Air Force Academy
Colorado 80840

FJSRL
USAF Academy, Colorado 80840

APGC (PGBPS-12)
Eglin AFB, Florida 32542

AFETR Technical Library
(ETV, MU-135)
Patrick AFB, Florida 32925

AFETR (ETLLG-1)
STINFO Officer (for Library)
Patrick AFB, Florida 32925

ESD (ESTI)
L. G. Hanscom Field
Bedford, Massachusetts 01731

AEDC (ARO, INC)
Attn: Library/Documents
Arnold AFS, Tennessee 37389

European Office of Aerospace Research
Shell Building
47 Rue Cantersteen
Brussels, Belgium

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

Department of the Army

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

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

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

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

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

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

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

Commanding General
Frankford Arsenal
Attn: SMFA-L6000-64-4 (Dr. Sidney Ross)
Philadelphia, Pennsylvania 19137

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

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

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

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

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

Commanding Officer
Human Engineering Laboratories
Aberdeen Proving Ground, Maryland 21005

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

Commandant
U.S. Army Command and General
Staff College
Attn: Secretary
Fort Leavenworth, Kansas 66270

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

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

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

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

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

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

Dr. S. Benedict Levin, 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

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

AMSEL-RD-D	HL-O
RD-G	HL-R
RD-MAF-1	NL-D
RD-MAT	NL-A
RD-GF	NL-P
XL-D	NL-R
XL-E	NL-S
XL-C	KL-D
XL-S	KL-E
HL-D	KL-S
HL-L	KL-T
HL-J	VL-D
HL-P	WL-D

Department of the Navy

Chief of Naval Research
Department of the Navy
Washington, D.C. 20360
Attn: Code 427

Chief, Bureau of Ships
Department of the Navy
Washington, D.C. 20360

Chief, Bureau of Weapons
Department of the Navy
Washington, D.C. 20360

Commanding Officer
Office of Naval Research Branch Office
Box 39, Navy No 100 F.P.O.
New York, New York 09510

Commanding Officer
Office of Naval Research Branch Office
1030 East Green Street
Pasadena, California

Commanding Officer
Office of Naval Research Branch Office
219 South Dearborn Street
Chicago, Illinois 60604

Commanding Officer
Office of Naval Research Branch Office
207 West 42nd Street
New York, New York 10011

Commanding Officer
Office of Naval Research Branch Office
495 Summer Street
Boston, Massachusetts 02210

Director, Naval Research Laboratory
Technical Information Officer
Washington, D.C.
Attn: Code 2000

Commander
Naval Air Development and Material Center
Johnsville, Pennsylvania 18974

Librarian, U.S. Electronics Laboratory
San Diego, California 95152

Commanding Officer and Director
U.S. Naval Underwater Sound Laboratory
Fort Trumbull
New London, Connecticut 06840

Librarian, U.S. Naval Post Graduate School
Monterey, California

Commander
U.S. Naval Air Missile Test Center
Point Magu, California

Director
U.S. Naval Observatory
Washington, D.C.

Chief of Naval Operations
OP-07
Washington, D.C.

Director, U.S. Naval Security Group
Attn: G43
3801 Nebraska Avenue
Washington, D.C.

Commanding Officer
Naval Ordnance Laboratory
White Oak, Maryland

Commanding Officer
Naval Ordnance Laboratory
Corona, California

Commanding Officer
Naval Ordnance Test Station
China Lake, California

Commanding Officer
Naval Avionics Facility
Indianapolis, Indiana

Commanding Officer
Naval Training Device Center
Orlando, Florida

U.S. Naval Weapons Laboratory
Dahlgren, Virginia

Weapons Systems Test Division
Naval Air Test Center
Patuxtent River, Maryland
Attn: Library

Other Government Agencies

Mr. Charles F. Yost
Special Assistant to the Director
of Research
NASA
Washington, D.C. 20546

NASA Lewis Research Center
Attn: Library
21000 Brookpark Road
Cleveland, Ohio 44135

Dr. H. Harrison, Code RRE
Chief, Electrophysics Branch
NASA, Washington, D.C. 20546

Goddard Space Flight Center
NASA
Attn: Library, Documents Section Code 252
Green Belt, Maryland 20771

National Science Foundation
Attn: Dr. John R. Lehmann
Division of Engineering
1800 G Street N.W.
Washington, D.C. 20550

U.S. Atomic Energy Commission
Division of Technical Information Extension
P.O. Box 62
Oak Ridge, Tennessee 37831

Los Alamos Scientific Library
Attn: Reports Library
P.O. Box 1663
Los Alamos, New Mexico 87544

NASA Scientific & Technical Information
Facility
Attn: Acquisitions Branch (S/AK/DL)
P.O. Box 33
College Park, Maryland 20740

Non-Government Agencies

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

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

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

Director
Stanford Electronics Laboratories
Stanford University
Stanford, California

Director
Coordinated Science Laboratory
University of Illinois
Urbana, Illinois 61803

Director
Electronics Research Laboratory
University of California
Berkeley 4, California

Director
Electronics Sciences Laboratory
University of Southern California
Los Angeles, California 90007

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

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

Aerospace Corporation
P.O. Box 95085
Los Angeles, California 90045
Attn: Library Acquisitions Group

Professor Nicholas George
California Institute of Technology
Pasadena, California

Aeronautics Library
Graduate Aeronautical Laboratories
California Institute of Technology
1201 E. California Blvd.
Pasadena, California 91109

Director, USAF Project RAND
Via: Air Force Liaison Office
The RAND Corporation
1700 Main Street
Santa Monica, California 90406
Attn: Library

The Johns Hopkins University
Applied Physics Laboratory
8621 Georgia Avenue
Silver Spring, Maryland
Attn: Boris W. Kuvshinoff
Document Librarian

School of Engineering Sciences
Arizona State University
Tempe, Arizona

Dr. Leo Young
Stanford Research Institute
Menlo Park, California

Hunt Library
Carnegie Institute of Technology
Schenley Park
Pittsburgh, Pennsylvania 15213

Mr. Henry L. Bachmann
Assistant Chief Engineer
Wheeler Laboratories
122 Cuttermill Road
Great Neck, New York

University of Liege
Electronic Institute
15, Avenue Des Tilleuls
Val-Benoit, Liege
Belgium

University of California at Los Angeles
Department of Engineering
Los Angeles, California

California Institute of Technology
Pasadena, California
Attn: Documents Library

University of California
Santa Barbara, California
Attn: Library

Carnegie Institute of Technology
Electrical Engineering Department
Pittsburgh, Pennsylvania

University of Michigan
Electrical Engineering Department
Ann Arbor, Michigan

New York University
College of Engineering
New York, New York

Syracuse University
Dept. of Electrical Engineering
Syracuse, New York

Yale University
Engineering Department
New Haven, Connecticut

Bendix Pacific Division
11600 Sherman Way
North Hollywood, California

General Electric Company
Research Laboratories
Schenectady, New York

Airborne Instruments Laboratory
Deerpark, New York

Lockheed Aircraft Corporation
P.O. Box 504
Sunnyvale, California

Raytheon Company
Bedford, Massachusetts
Attn: Librarian

UNCLASSIFIED

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) Research Laboratory of Electronics Massachusetts Institute of Technology Cambridge, Massachusetts	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b GROUP

3. REPORT TITLE

Error Bounds for Parallel Communication Channels

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

Technical Report

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

Ebert, Paul M.

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
August 1, 1966	100	27

8a. CONTRACT OR GRANT NO. DA36-039-AMC-03200(E) b. PROJECT NO. 200-14501-B31F NSF Grant GP-2495 c. NIH Grant MH-04737-05 NASA Grant NsG-334, NsG-496 d.	9a. ORIGINATOR'S REPORT NUMBER(S) Technical Report 448 9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)

10. AVAILABILITY/LIMITATION NOTICES

Distribution of this document is unlimited

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY Joint Services Electronics Program thru USAECOM, Fort Monmouth, N.J.

13. ABSTRACT

This report is concerned with the extension of known bounds on the achievable probability of error with block coding to several types of paralleled channel models.

One such model is that of non-white additive gaussian noise. We are able to obtain upper and lower bounds on the exponent of the probability of error with an average power constraint on the transmitted signals. The upper and lower bounds agree at zero rate and for rates between a certain R_{crit} and the capacity of the channel. The surprising result is that the appropriate bandwidth used for transmission depends only on the desired rate and not on the power or exponent desired over the range wherein the upper and lower bounds agree.

We also consider the problem of several channels in parallel with the option of using separate coders and decoders on the parallel channels. We find that there are some cases in which there is a saving in coding and decoding equipment by coding for the parallel channels separately. We determine the asymptotic ratio of the optimum blocklength for the parallel channels and analyze one specific coding scheme to determine the effect of rate and power distribution among the parallel channels.

DD FORM 1 JAN 64 1473

UNCLASSIFIED

Security Classification

UNCLASSIFIED
Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Parallel Communication Channels, Error Bounds Block Coding Parallel Channels, separate coders and decoders						

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.

2*a*. 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.

2*b*. 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.

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

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

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

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

9*a*. 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.

9*b*. 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, rules, and weights is optional.

UNCLASSIFIED
Security Classification