INFORMATION AND CONTROL 10, 65–103 (1967)

# Lower Bounds to Error Probability for Coding on Discrete Memoryless Channels. I

C. E. SHANNON* AND R. G. GALLAGER*

*Departments of Electrical Engineering and Mathematics, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts*

AND

E. R. BERLEKAMP†

*Department of Electrical Engineering, University of California, Berkeley, California*

New lower bounds are presented for the minimum error probability that can be achieved through the use of block coding on noisy discrete memoryless channels. Like previous upper bounds, these lower bounds decrease exponentially with the block length $N$. The coefficient of $N$ in the exponent is a convex function of the rate. From a certain rate of transmission up to channel capacity, the exponents of the upper and lower bounds coincide. Below this particular rate, the exponents of the upper and lower bounds differ, although they approach the same limit as the rate approaches zero. Examples are given and various incidental results and techniques relating to coding theory are developed. The paper is presented in two parts: the first, appearing here, summarizes the major results and treats the case of high transmission rates in detail; the second, to appear in the subsequent issue, treats the case of low transmission rates.

## I. INTRODUCTION AND SUMMARY OF RESULTS

The noisy channel coding theorem (Shannon, 1948) states that for a broad class of communication channels, data can be transmitted over the channel in appropriately coded form at any rate less than channel

* The work of these authors was supported by the National Aeronautics and Space Administration (Grants NsG-334 and NsG-496), the Joint Services Electronics Program (contract DA-36-039-AMC-03200 (EE)), and the National Science Foundation (Grant GP-2495).

† The work of this author is supported by the Air Force Office of Scientific Research (Grant, AF-AFOSR-639-65).

capacity with arbitrarily small error probability. Naturally there is a rub in such a delightful sounding theorem, and the rub here is that the error probability can, in general, be made small only by making the coding constraint length large; this, in turn, introduces complexity into the encoder and decoder. Thus, if one wishes to employ coding on a particular channel, it is of interest to know not only the capacity but also how quickly the error probability can be made to approach zero with increasing constraint length. Feinstein (1955), Shannon (1958), Fano (1961), and Gallager (1965) have shown that for discrete memoryless channels, block coding and decoding schemes exist for which the error probability approaches zero exponentially with increasing block length for any given data rate less than channel capacity.

This paper is concerned primarily with the magnitude of this exponential dependence. We derive some lower bounds on achievable error probability, summarized in Theorems 1 to 4 below, and compare these bounds with the tightest known general upper bounds on error probability.

A *discrete channel* is a channel for which the input and output are sequences of letters from finite alphabets. Without loss of generality, we can take the input alphabet to be the set of integers $(1, \cdots, K)$ and the output alphabet to be the set of integers $(1, \cdots, J)$. A *discrete memoryless channel* is a discrete channel in which each letter of the output sequence is statistically dependent only on the corresponding letter of the input sequence. A discrete memoryless channel is specified by its set of transition probabilities $P(j \mid k)$, $1 \leqq j \leqq J$, $1 \leqq k \leqq K$, where $P(j \mid k)$ is the probability of receiving digit $j$ given that digit $k$ was transmitted. If $\mathbf{x} = (k_1, k_2, \cdots, k_N)$ is a sequence of $N$ input letters and $\mathbf{y} = (j_1, \cdots, j_N)$ is a corresponding sequence of $N$ output letters, then for a memoryless channel

$$\Pr(\mathbf{y} \mid \mathbf{x}) = \prod_{n=1}^{N} P(j_n \mid k_n) \tag{1.1}$$

A *block code* with $M$ code words of length $N$ is a mapping from a set of $M$ *source messages*, denoted by the integers 1 to $M$, onto a set of $M$ *code words*, $\mathbf{x}_1, \cdots, \mathbf{x}_M$, where each code word is a sequence of $N$ letters from the channel input alphabet. A *decoding scheme* for such a code is a mapping from the set of output sequences of length $N$ into the integers 1 to $M$. If the source attempts to transmit message $m$ over the channel via this coding and decoding scheme, message $m$ is encoded into sequence $\mathbf{x}_m$;

after transmitting $\mathbf{x}_m$, some sequence $\mathbf{y}$ is received which is mapped into an integer $m'$. If $m' \neq m$, we say that a decoding error has occurred.

It is convenient here to consider a somewhat more general problem, *list decoding*, where the decoder, rather than mapping the received sequence into a single integer, maps it into a list of integers each between 1 and $M$. If the transmitted source message is not on the list of decoded integers, we say that a *list decoding error* has occurred.

List decoding was first considered by Elias (1955) for the Binary Symmetric Channel. Most of the known bounds on error probability extend readily with simple alterations to list decoding and the concept has been very useful both in providing additional insight about ordinary decoding and as a tool in proving theorems (see, for example, Jacobs and Berlekamp (1967)).

For a given code and list decoding scheme, let $Y_m$ be the set of received sequences for which message $m$ is on the list of decoded integers and let $Y_m{}^c$ be the complement of the set $Y_m$. Then the probability of a list decoding error, given that the source message is $m$, is the conditional probability that $\mathbf{y}$ is in $Y_m{}^c$, or

$$P_{e,m} = \sum_{\mathbf{y} \in Y_m{}^c} \Pr(\mathbf{y} \mid \mathbf{x}_m) \tag{1.2}$$

The error probability for a given code and list decoding scheme is then defined as the average $P_{e,m}$ over $m$ assuming that the messages are equally likely,

$$P_e = \frac{1}{M} \sum_{m=1}^{M} P_{e,m} \tag{1.3}$$

We define $P_e(N, M, L)$ as the minimum error probability for the given channel minimized over all codes with $M$ code words of length $N$ and all list decoding schemes where the size of the list is limited to $L$. $P_e(N, M, 1)$ is thus the minimum error probability using ordinary decoding. Finally the *rate* $R$ of a code with list decoding is defined as

$$R = \frac{\ln M/L}{N} = \frac{\ln M}{N} - \frac{\ln L}{N} \tag{1.4}$$

For ordinary decoding where $L = 1$, this is the usual definition of rate and is the source entropy per channel digit for equally likely messages. For larger $L$, we may think of $(\ln L)/N$ as a correction term to account for the fact that the receiver is only asserting the message to be one of a

list of $L$. For example, if $M = L$, (1.4) asserts that $R = 0$, and indeed no channel is required.

With these definitions, we can proceed to summarize the major results of the paper. The major result of Section II is Theorem 1 below, which lower bounds the error probability of a code in terms of the minimum achievable error probability at 2 shorter blocklengths.

THEOREM 1. *Let $N_1$, $N_2$ be arbitrary blocklengths and let $M$, $L_1$, and $L_2$ be arbitrary positive integers. Then the minimum error probability achievable for a code of $M$ code words of length $N_1 + N_2$ is bounded by*

$$P_e(N_1 + N_2, M, L_2) \geqq P_e(N_1, M, L_1)P_e(N_2, L_1 + 1, L_2) \quad (1.5)$$

In Section VI this theorem leads directly to an exponential type lower bound on error probability which for low transmission rates is considerably tighter than any previously known bound.

In Section III, codes containing only two code words are analyzed in detail. We find the trade-offs between the error probability when the first word is sent and the error probability when the second word is sent. The results, which are used in Sections IV and V, are summarized in Section III by Theorem 5 and Fig. 3.1.

The major result of Section IV is the "sphere packing" bound on error probability, given below as Theorem 2. This theorem, in slightly different form, was discovered by Fano (1961) but has not been rigorously proven before.

THEOREM 2. *Given a discrete memoryless channel with transition probabilities $P(j \mid k)$; $1 \leqq k \leqq K$, $1 \leqq j \leqq J$; $P_e(N, M, L)$ is lower bounded by*

$$P_e(N, M, L) \geqq \exp - N\{E_{sp}[R - o_1(N)] + o_2(N)\} \quad (1.6)$$

*where the function $E_{sp}$ is defined by*

$$E_{sp}(R) = \underset{\rho \geqq 0}{\text{L.U.B.}} [E_0(\rho) - \rho R] \quad (1.7)$$

$$E_0(\rho) = \max_{\mathbf{q}} E_0(\rho, \mathbf{q}) \quad (1.8)$$

$$E_0(\rho, \mathbf{q}) = -\ln \sum_{j=1}^{J} \left[ \sum_{k=1}^{K} q_k P(j \mid k)^{1/(1+\rho)} \right]^{1+\rho} \quad (1.9)$$

*The maximum in (1.8) is over all probability vectors $\mathbf{q} = (q_1, \cdots, q_K)$; that is, over all $\mathbf{q}$ with nonnegative components summing to 1. The quantities $o(N)$ go to 0 with increasing $N$ and can be taken as*

$$o_1(N) = \frac{\ln 8}{N} + \frac{K \ln N}{N} \quad \text{and} \quad o_2(N) = \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} + \frac{\ln 8}{N} \tag{1.10}$$

*where $P_{\min}$ is the smallest nonzero $P(j \mid k)$ for the channel and $K$ and $J$ are the sizes of the input and output alphabets respectively.*

The quantity in braces in (1.6) can be found graphically from $E_{sp}(R)$ by taking each point on the $E_{sp}(R)$ curve, moving to the right $o_1(N)$ and moving upward $o_2(N)$. Thus the major problem in understanding the implication of the theorem is understanding the behavior of $E_{sp}(R)$. Figure 1 sketches $E_{sp}(R)$ for a number of channels. Figure 1(a) is the typical behavior; the other sketches are examples of the rather peculiar curves that can occur if some of the $P(j \mid k)$ are zero.

For a given $\rho$, $E_0(\rho) - \rho R$ is a linear function of $R$ with slope $-\rho$. Thus, as shown in Fig. 2, $E_{sp}(R)$ is the least upper bound of this family of straight lines. It is obvious geometrically, and easy to prove analytically, that $E_{sp}(R)$ is nonincreasing in $R$ and is convex $\cup$[1] (see Fig. 2). It is shown in the appendix that $E_{sp}(R) = 0$ for $R \geqq C$ where $C$ is channel capacity and that $E_{sp}(R) > 0$ for $0 \leqq R < C$. It sometimes happens that $E_{sp}(R) = \infty$ for sufficiently small values of $R$ (see Fig. 1(b), (c), (d), (e)). To investigate this, we observe that for fixed $\rho$, $E_0(\rho) - \rho R$ intercepts the $R$ axis at $E_0(\rho)/\rho$. As $\rho \to \infty$ this line will approach a vertical line at $R = \lim_{\rho \to \infty} E_0(\rho)/\rho$ (see Fig. 2(b)). This limiting rate is called $R_\infty$ and $E_{sp}(R)$ is finite for $R \geqq R_\infty$ and infinite for $R < R_\infty$.

$$R_\infty = \lim_{\rho \to \infty} \max_{\mathbf{q}} \frac{-\ln \sum_j \left[\sum_k q_k P(j \mid k)^{1/(1+\rho)}\right]^{1+\rho}}{\rho}$$

Finding the limit either by expanding in a Taylor series in $1/(1+\rho)$ or by using L'Hospitals rule,

$$R_\infty = \max_{\mathbf{q}} - \ln \max_{1 \leqq j \leqq J} \sum_k q_k \varphi(j \mid k) \tag{1.11}$$

$$\varphi(j \mid k) = \begin{cases} 1; & P(j \mid k) \neq 0 \\ 0; & P(j \mid k) = 0 \end{cases}$$

[1] We will use convex $\cup$ (read convex cup) and concave $\cap$ (concave cap) as mnemonic aids to the reader for convex and concave functions. It seems as difficult for the nonspecialist to remember which is which as to remember the difference between stalagmites and stalactites.

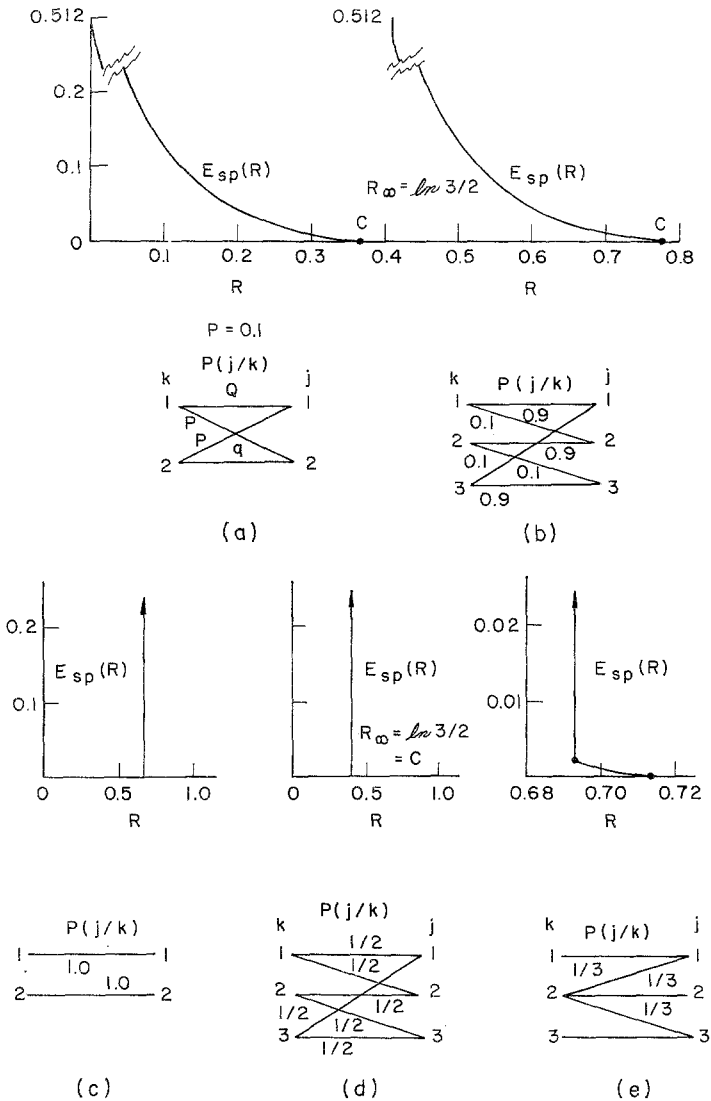


FIG. 1. The sphere packing exponent for several channels.

That is, for each output, we sum the input probabilities $q_k$ that lead to that output. We then adjust the $q_k$ to minimize the largest of these sums; $R_\infty$ is minus the logarithm of that min-max sum. It can be seen from this that $R_\infty > 0$ iff each output is unreachable from at least one input.

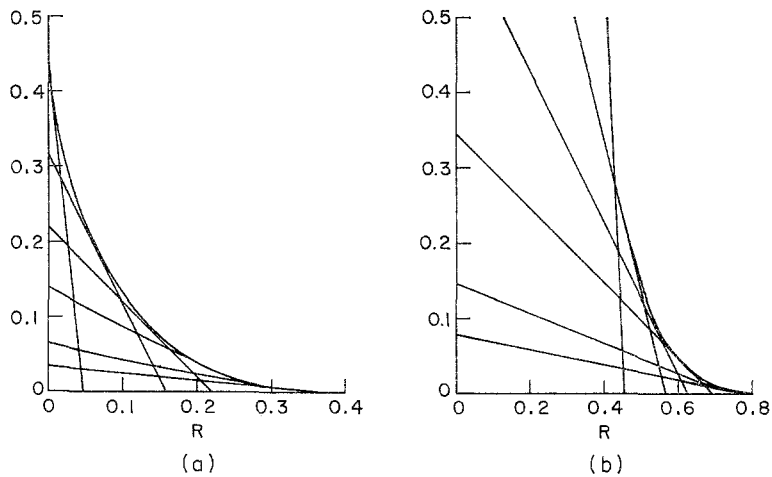


FIG. 2. $E_{sp}(R)$ as convex hull of straight lines (same channels as Fig. 1).

$R_\infty$ is an upper bound to the zero error capacity of the channel, $C_0$. Shannon (1956) has defined $C_0$ as the least upper bound of rates at which information can be transmitted with no possibility of errors. $C_0$ is greater than 0 iff there are two or more inputs from which no common output can be reached and thus it is possible to have $R_\infty > 0$ and $C_0 = 0$ (see Fig. 1(b) for such a channel). Shannon (1956) has shown that if $C_0 > 0$, then the expression in (1.11) for $R_\infty$ is equal to the zero error capacity of the channel with noiseless feedback.

If it happens that $R_\infty$ equals channel capacity $C$, then the sphere packing bound merely states the true but uninteresting result that $P_e \geqq 0$ for $R < C$. It is shown in the appendix that this occurs iff the following relations are satisfied for the input probability assignment $\mathbf{q} = (q_1, \cdots, q_K)$ that yields capacity.

(a) All transition probabilities that lead to a given output with nonzero probability are the same (i.e., $P(j \mid k)$ is independent of $k$ for those $j, k$ such that $q_k P(j \mid k) \neq 0$).

(b) The sum of the $q_k$ over inputs leading to a given output $j$ is independent of the output $j$.

These conditions are satisfied by all noiseless channels and also a few noisy channels such as that in Fig. 1(c). For all other channels, $R_\infty < C$. It is shown in the appendix that $E_{sp}(R)$ is strictly convex $\cup$ and strictly

decreasing in this region. $E_{sp}(\mathrm{R})$ need not have a continuous derivative however (see Gallager (1965), Fig. 6).

The sphere packing bound above bears a striking resemblance to the "random coding" *upper* bound on error probability of Fano (1961) and Gallager (1965). That bound, as stated by Gallager, is

$$P_e(N, M, 1) \leqq \exp - NE_r(R) \tag{1.12}$$

where

$$E_r(R) = \max_{0 \leqq \rho \leqq 1} [E_0(\rho) - \rho R] \tag{1.13}$$

Comparing $E_r(R)$ and $E_{sp}(R)$, we see that $E_{sp}(R) \geqq E_r(R)$. Equality holds iff the value of $\rho \geqq 0$ that maximizes $E_0(\rho) - \rho R$ is between 0 and 1. It can be seen from Fig. 2 that the value of $\rho \geqq 0$ that maximizes $E_0(\rho) - \rho R$ is nonincreasing with $R$. Consequently there exists a number called the *critical rate*, $R_{\text{crit}}$, such that $E_{sp}(R) = E_r(R)$ iff $R \geqq R_{\text{crit}}$. $R_{\text{crit}}$ lies between $R_\infty$ and $C$ and it is shown in the appendix that $R_{\text{crit}} = C$ iff $R_\infty = C$ (i.e., if conditions (a) and (b) above are satisfied). For all other channels there is a nonzero range of rates, $R_{\text{crit}} \leqq R \leqq C$, where the upper and lower bounds on error probability agree except for the $o(N)$ terms (see Fig. 3).

This completes our discussion of Theorem 2. For a more complete discussion of how to calculate $E_{sp}(R)$ and $E_r(R)$ see Gallager (1965). One additional result needed here, however, is the following (Gallager (1965), Theorem 4): any local maximum of (1.8) over the probability vector $\mathbf{q}$ is a global maximum, and necessary and sufficient conditions on $\mathbf{q}$ to maximize (1.8) for a given $\rho$ are

$$\sum_j [P(j \mid k)]^{1/(1+\rho)} \alpha_j^{\rho} \geqq \sum_j \alpha_j^{1+\rho} \quad \text{for all} \quad k, 1 \leqq k \leqq K \tag{1.14}$$

where

$$\alpha_j = \sum_k q_k [P(j \mid k)]^{1/(1+\rho)} \tag{1.15}$$

Equation (1.14) must be satisfied with equality except for those $k$ for which $q_k = 0$; this can be seen by multiplying both sides of (1.14) by $q_k$ and summing over $k$.

In Section V (contained in Part II) we find bounds on error probability for codes with a fixed number of code words in the limit as the block length becomes large. The exponent $E_M$ for a code with $M$ code

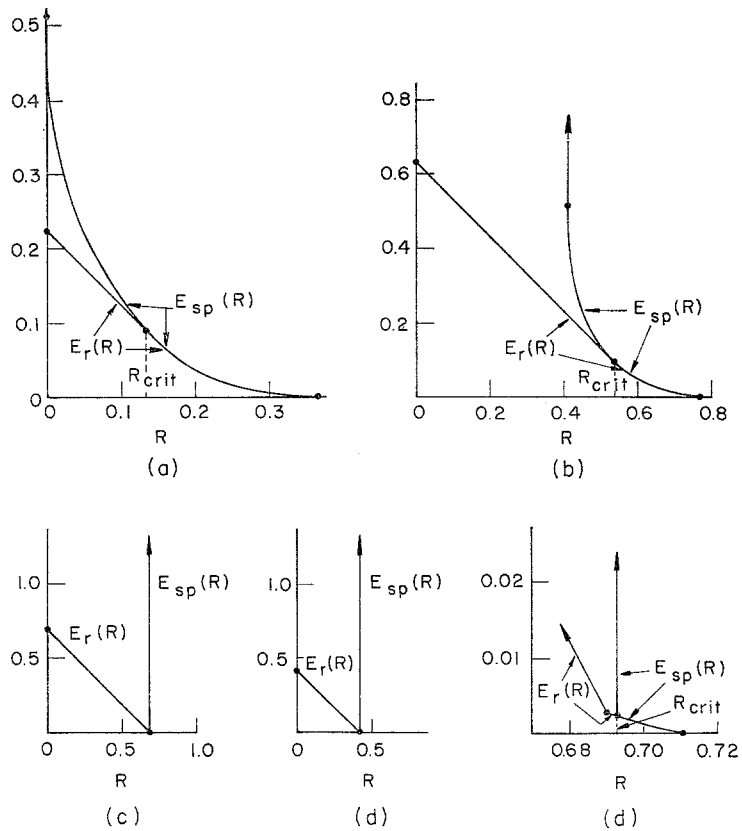


FIG. 3. Comparison of sphere packing exponent with random coding exponent (same channels as Fig. 1).

words is defined as

$$E_M = \lim_{N\to\infty} \sup \frac{-\ln P_e(N, M, 1)}{N} \tag{1.16}$$

The major result of the section is the following theorem concerning the exponents, $E_M$.

THEOREM 3. *Given a discrete memoryless channel with transition probabilities* $P(j \mid k)$; $1 \leqq k \leqq K$, $1 \leqq j \leqq J$, *and given that the zero error capacity is zero,* $P_e(N, M, 1)$ *is lower bounded by*

$$P_e(N, M, 1) \geqq \exp - N[E_M + o_3(N)] \tag{1.17}$$

*The exponents approach a limit,* $E_\infty = \lim_{M\to\infty} E_M$, *given by*

$$E_\infty = \max_{\mathbf{q}} -\sum_{i=1}^{K}\sum_{k=1}^{K} q_i q_k \ln \sum_{j=1}^{J} \sqrt{P(j\,|\,i)P(j\,|\,k)} \tag{1.18}$$

*The maximum in* (1.18) *is over all probability vectors* $\mathbf{q} = (q_1, \cdots, q_K)$. *The exponents* $E_M$ *are bounded by*

$$E_\infty \leqq E_M \leqq E_\infty + 2\sqrt{K}A/\sqrt{[\log_2 (\log_2 M)]^-} \tag{1.19}$$

*where*

$$A = \max_{i,k} -2 \ln \sum_{j=1}^{J} \sqrt{P(j\,|\,i)P(j\,|\,k)} \tag{1.20}$$

*and* $[x]^-$ *denotes the largest integer less than or equal to* $x$. *The quantity* $o_3(N)$ *in* (1.17) *can be taken as*

$$o_3(N) = \frac{\ln 4M}{N} - \sqrt{\frac{2}{N}} \ln P_{\min} \tag{1.21}$$

*where* $P_{\min}$ *is the smallest nonzero* $P(j\,|\,k)$.

Theorem 3 again requires some interpretation. Since $C_0 = 0$ by assumption, every pair of inputs has at least one output in common so that $\sum_{j=1}^{J} \sqrt{P(j\,|\,i)P(j\,|\,k)} > 0$ for all $i$, $k$; thus $E_\infty$ and $A$ in (1.18) and (1.20) must be finite.

Each of the exponents $E_M$ can be interpreted as an exponent corresponding to zero rate since for fixed $M$, the rate of a code $R = (\ln M)/N$ approaches zero as $N$ approaches infinity. On the other hand, if we choose $M$ as a function of $N$ in such a way that $\lim_{N\to\infty} M(N) = \infty$; $\lim_{N\to\infty} (\ln M(N))/N = 0$, then (1.17) becomes

$$P_e(N, M(N), 1) \geqq \exp -N[E_\infty + o_4(N)] \tag{1.22}$$

where $o_4(N)$ approaches zero as $N$ approaches infinity.

For channels with a symmetry condition called pairwise reversibility, the exponents $E_M$ can be uniquely determined. A channel is defined to be pairwise reversible iff for each pair of inputs, $i$ and $k$,

$$\sum_{j=1}^{J} \sqrt{P(j\,|\,k)P(j\,|\,i)} \ln P(j\,|\,k) = \sum_{j=1}^{J} \sqrt{P(j\,|\,k)P(j\,|\,i)} \ln P(j\,|\,i) \tag{1.23}$$

This condition will be discussed more fully in Section V, but it is satis-

fied by such common channels as the binary symmetric channel and the binary symmetric erasure channel. For any channel satisfying (1.23), it is shown that

$$E_M = \frac{M}{M-1} \max_{M_1,\cdots,M_K} - \sum_i \sum_k \frac{M_i}{M} \frac{M_k}{M} \ln \sum_j \sqrt{P(j \mid i) P(j \mid k)} \quad (1.24)$$

where the $M_k \geqq 0$ are integers summing to $M$.

In Section VI, Theorems 1, 2, and 3 are combined to yield a new lower bound on error probability. The sphere packing bound is applied to $P_e(N_1, M, L)$ in (1.5) and the zero rate bound is applied to $P_e(N_2, L+1, 1)$. The result is given by the following theorem.

THEOREM 4. *Let $E_{sp}(R)$ and $E_\infty$ be given by* (1.7) *and* (1.18) *for an arbitrary discrete memoryless channel for which $C_0 = 0$. Let $E_{sl}(R)$ be the smallest linear function of $R$ which touches the curve $E_{sp}(R)$ and which satisfies $E_{sl}(0) = E_\infty$. Let $R_1$ be the point where $E_{sl}(R)$ touches $E_{sp}(R)$. Then for any code with a rate $R < R_1$,*

$$P_e(N, M, 1) \geqq \exp - N[E_{sl}(R - o_5(N)) + o_6(N)] \quad (1.25)$$

*where $o_5(N)$ and $o_6(N)$ are given by* (6.6) *and* (6.7) *and approach zero as $N$ approaches infinity.*

The function $E_{sl}(R)$ is sketched for a number of channels in Fig. 4. $E_\infty$ is always strictly less than $E_{sp}(0^+)$ unless channel capacity $C$ is zero. Thus the straight line bound of Theorem 4 is always tighter than the sphere packing bound at low rates for sufficiently large block lengths whenever $C > 0$, $C_0 = 0$.

Theorem 4 can be compared with an upper bound to error probability derived by Gallager (1965, Theorem 6) using expurgated randomly chosen codes. That result states that for any $N$, $M$,

$$P_e(N, M, 1) \leqq \exp - N \left[ E_{ex}\left(R + \frac{\ln 4}{N}\right)\right] \quad (1.26)$$

where the function $E_{ex}$ is given by

$$E_{ex}(R) = \underset{\rho \geqq 1}{\text{L.U.B.}} [E_x(\rho) - \rho R] \quad (1.27)$$

$$E_x(\rho) = \max_{\mathbf{q}} - \rho \ln \sum_{k=1}^{K} \sum_{i=1}^{K} q_k q_i \left[ \sum_{j=1}^{J} \sqrt{P(j \mid k) P(j \mid i)} \right]^{1/\rho} \quad (1.28)$$

The maximization in (1.28) is again over probability vectors $\mathbf{q}$.

The function $E_{ex}(R)$ is sketched for several channels in Fig. 4. It can

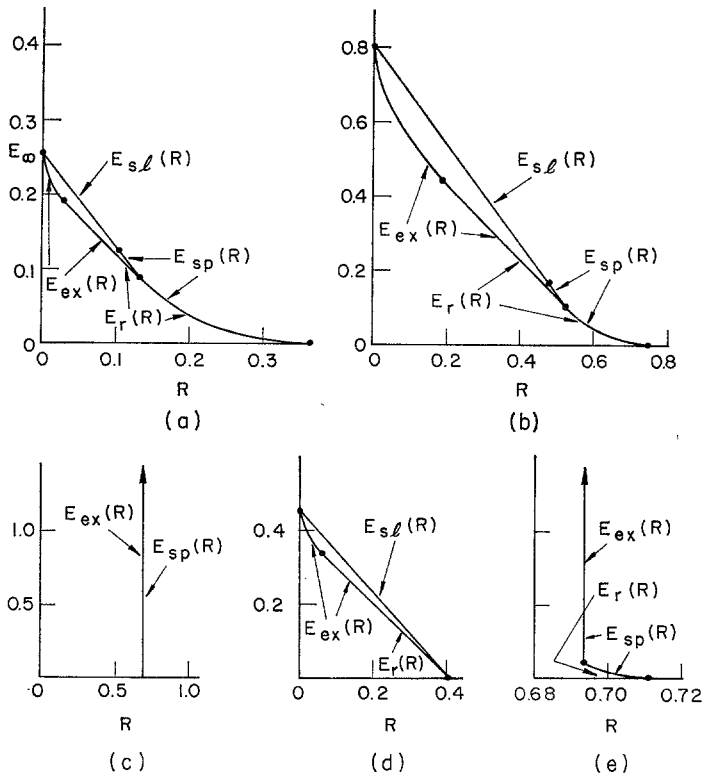


FIG. 4. Bounds on reliability function (same channels as Fig. 1)

be interpreted as the least upper bound of a set of straight lines where the lines have slope $-\rho$ and zero intercept $E_x(\rho)$. The function $E_x(\rho)$ is increasing with $\rho$ and if $C_0 = 0$, we can calculate $\lim_{\rho\to\infty} E_x(\rho)$ as

$$\lim_{\rho\to\infty} E_x(\rho) = \max_{\mathbf{q}} \sum_{k=1}^{K}\sum_{i=1}^{K} q_k q_i \ln \sum_{j=1}^{J} \sqrt{P(j\,|\,k)P(j\,|\,i)} \qquad (1.29)$$

Also it can be seen from (1.27) that

$$\lim_{R\to 0} E_{ex}(R) = \lim_{\rho\to\infty} E_x(\rho) \qquad (1.30)$$

Combining (1.18), (1.29), and (1.30), we see that

$$\lim_{R\to 0} E_{ex}(R) = E_\infty \qquad (1.31)$$

Thus, in the limit as $R \to 0$ our upper and lower bounds on $P_e$ have the same exponential dependence on the block length.

It is to be observed that all the upper and lower bounds to error probability discussed so far have an exponential dependence on block length for fixed rate. The correct value of this exponential dependence, as a function of rate, is of fundamental importance in coding theory and is defined as the *reliability function*, $E(R)$, of the channel. More precisely,

$$E(R) = \lim_{N \to \infty} \sup \frac{-\ln P_e(N, [e^{NR}]^+, 1)}{N} \tag{1.32}$$

where $[x]^+$ is the smallest integer greater than or equal to $x$. We see that $E_{sp}(R)$ and $E_{sl}(R)$ are upper bounds to $E(R)$, and $E_r(R)$ and $E_{ex}(R)$ are lower bounds. The bounds are identical for the rather uninteresting case of noiseless channels and for some rather peculiar channels such as Fig. 1(e), but for typical channels there is a region of uncertainty for rates between 0 and $R_{\text{crit}}$. Although the bounds are close enough to give considerable insight into the behavior of a channel with coding, it is still interesting to speculate on the value of $E(R)$ in this region of uncertainty, $0 < R \leqq R_{\text{crit}}$. For the binary symmetric channel, we improve on $E_{sl}(R)$ in Section VI by using a bound on minimum distance derived by Elias, but the technique does not generalize to arbitrary discrete memoryless channels. The authors would all tend to conjecture that $E(R)$ is equal to $E_{ex}(R)$ for $R \leqq R_{\text{crit}}$ if the maximization in (1.29) is performed on a block basis rather than a letter basis (i.e., using $\Pr(\mathbf{y} \mid \mathbf{x})$ in place of $P(j \mid k)$ and $q(\mathbf{x})$ in place of $q$) (see Gallager (1965)). As yet there is little concrete evidence for this conjecture.

## II. PROOF OF THEOREM 1

Theorem 1 establishes a lower bound on error probability for a code in terms of the error probabilities for two codes of shorter block lengths. Let $N_1$ and $N_2$ be arbitrary block lengths and consider a code with $M$ code words of block length $N_1 + N_2$. We shall be interested in considering each code word as consisting of two subsequences, the first of length $N_1$ and the second of length $N_2$. Let $\mathbf{x}_m$ be the $m$th code word and let the *prefix* $\mathbf{x}_{m,1}$ be the first $N_1$ letters of $\mathbf{x}_m$ and let the *suffix* $\mathbf{x}_{m,2}$ be the final $N_2$ letters of $\mathbf{x}_m$. Likewise, we separate the received sequence $\mathbf{y}$ into the prefix $\mathbf{y}_1$ and the suffix $\mathbf{y}_2$, consisting of $N_1$ and $N_2$ letters respectively.

We can visualize a list decoder of size $L_2$ as first observing $\mathbf{y}_1$, then $\mathbf{y}_2$, and decoding on the basis of these observations. Suppose that on the

basis of $\mathbf{y}_1$ alone, there is a given number, say $L_1$, of messages that are more likely at the decoder than the actual transmitted message. If $L_2$ of these $L_1$ messages are also more likely than the transmitted message on the basis of $\mathbf{y}_2$ above, then a list decoding error should surely be made. Reasoning heuristically, it appears that the probability of the first event above is the probability of a list decoding error for a code of $M$ code words of length $N_1$ with a list size of $L_1$. Similarly, given the first event, the probability of the second event should be lower bounded by the probability of a list decoding error for a code of block length $N_2$ consisting of the $L_1$ most likely messages plus the actual transmitted message. We thus conclude heuristically that

$$P_e(N_1 + N_2, M, L_2) \geqq P_e(N_1, M, L_1)P_e(N_2, L_1 + 1, L_2) \quad (2.1)$$

This is the result of Theorem 1, and we now turn to a rigorous proof.

For a given code with $M$ code words of length $N_1 + N_2$, and a list decoding scheme of size $L_2$, let $Y_m$ be the set of received sequences $\mathbf{y}$ for which message $m$ is on the decoding list. Also, for any given received prefix, $\mathbf{y}_1$, let $Y_{m,2}(\mathbf{y}_1)$ be the set of suffixes $\mathbf{y}_2$ for which $m$ is on the list when $\mathbf{y}_1\mathbf{y}_2$ is received. Using (1.2) and (1.3) the error probability for the code is given by

$$P_e = \frac{1}{M} \sum_{m=1}^{M} \sum_{\mathbf{y} \in Y_m{}^c} \Pr(\mathbf{y} \mid \mathbf{x}_m) \quad (2.2)$$

For a discrete memoryless channel, $\Pr(\mathbf{y} \mid \mathbf{x}_m) = \Pr(\mathbf{y}_1 \mid \mathbf{x}_{m,1}) \Pr(\mathbf{y}_2 \mid \mathbf{x}_{m,2})$ and we can rewrite (2.2) as

$$P_e = \frac{1}{M} \sum_{m=1}^{M} \sum_{\mathbf{y}_1} \Pr(\mathbf{y}_1 \mid \mathbf{x}_{m,1}) \sum_{\mathbf{y}_2 \in Y_{m,2}^c(\mathbf{y}_1)} \Pr(\mathbf{y}_2 \mid \mathbf{x}_{m,2}) \quad (2.3)$$

Now consider the set of code word suffixes, $\mathbf{x}_{1,2}, \cdots, \mathbf{x}_{m,2}, \cdots, \mathbf{x}_{M,2}$. Pick any subset of $L_1 + 1$ of the messages and consider the associated $L_1 + 1$ suffixes as a set of $L_1 + 1$ code words of block length $N_2$. For any given $\mathbf{y}_1$, the associated $L_1 + 1$ decoding regions $Y_{m,2}(\mathbf{y}_1)$ form a list decoding rule of size $L_2$. Presumably some suffixes $\mathbf{y}_2$ are mapped into fewer than $L_2$ messages from the given subset, so that this is not the best set of decoding regions, but it is certainly a valid set. Now $P_e(N_2, L_1 + 1, L_2)$ is a lower bound to the error probability for any set of $L_1 + 1$ code words of length $N_2$ with any list decoding scheme of size $L_2$, and at least one code word in any such code must have an error probability that large. Thus, for at least one value of $m$ in any given subset of $L_1 + 1$ suffixes,

we have

$$\sum_{\mathbf{y}_2 \in Y^c_{m,2}(\mathbf{y}_1)} \Pr(\mathbf{y}_2 \mid \mathbf{x}_{m,2}) \geqq P_e(N_2, L_1 + 1, L_2) \tag{2.4}$$

For any given $\mathbf{y}_1$, consider the entire set of $M$ messages again. Let $m_1(\mathbf{y}_1), m_2(\mathbf{y}_1), \cdots, m_l(\mathbf{y}_1)$ be the set of messages for which (2.4) is *not* satisfied. This set must contain at most $L_1$ messages since otherwise we would have a subset of $L_1 + 1$ messages for which no member satisfied (2.4). We can then lower bound the left hand side of (2.4) for any $m$ by

$$\sum_{\mathbf{y}_2 \in Y^c_{m,2}(\mathbf{y}_1)} \Pr(\mathbf{y}_2 \mid \mathbf{x}_{m,2}) \geqq \begin{cases} 0; & m = m_1(\mathbf{y}_1), \cdots, m_l(\mathbf{y}_1) \\ P_e(N_2, L_1 + 1, L_2); & m \neq m_1(\mathbf{y}_1), \cdots, m_l(\mathbf{y}_1) \end{cases} \tag{2.5}$$

where $l$ depends on $\mathbf{y}_1$ but always satisfies $l \leqq L_1$.

Interchanging the order of summation between $m$ and $\mathbf{y}_1$ in (2.3) and substituting (2.5) into (2.3), we obtain

$$P_e \geqq \frac{1}{M} \sum_{\mathbf{y}_1} \sum_{\substack{m \neq m_i(\mathbf{y}_1) \\ i=1,\cdots,l}} \Pr(\mathbf{y}_1 \mid \mathbf{x}_{m,1}) P_e(N_2, L_1 + 1, L_2) \tag{2.6}$$

$$P_e \geqq P_e(N_2, L_1 + 1, L_2) \left[ \frac{1}{M} \sum_{\mathbf{y}_1} \sum_{\substack{m \neq m_i(\mathbf{y}_1) \\ i=1,\cdots,l}} \Pr(\mathbf{y}_1 \mid \mathbf{x}_{m,1}) \right] \tag{2.7}$$

Finally, to complete the proof, we can consider the set of prefixes $\mathbf{x}_{1,1}, \cdots, \mathbf{x}_{M,1}$ as a set of $M$ code words of length $N_1$, and the sets $m_1(\mathbf{y}_1), \cdots, m_l(\mathbf{y}_1)$ as a list decoding rule of size $L_1$ (recall that $l \leqq L_1$ for all $\mathbf{y}_1$). Let $Y_{m,1}$ be the set of $\mathbf{y}_1$ for which $m$ is on the list $\mathrm{m}_1(\mathbf{y}_1), \cdots, m_l(\mathbf{y}_1)$. Interchanging the sum over $m$ and $\mathbf{y}_1$ in (2.7), we obtain

$$P_e \geqq P_e(N_2, L_1 + 1, L_2) \left[ \frac{1}{M} \sum_{m=1}^{M} \sum_{\mathbf{y}_1 \in Y^c_{m,1}} \Pr(\mathbf{y}_1 \mid \mathbf{x}_{m,1}) \right] \tag{2.8}$$

The quantity in brackets is the probability of list decoding error for this code of length $N_1$ and is lower bounded by $P_e(N_1, M, L_1)$

$$P_e \geqq P_e(N_2, L_1 + 1, L_2) P_e(N_1, M, L_1) \tag{2.9}$$

Thus any code with $M$ code words of length $N_1 + N_2$ and any list decoding scheme of size $L_2$ has an error probability satisfying (2.9) and this establishes (2.1).

The above theorem can be generalized considerably. First we note that the assumption of a discrete channel was used only in writing sums over the output sequences. For continuous channels, these sums are replaced by integrals. The theorem can also be modified to apply to a broad class of channels with memory. Also, if there is feedback from the receiver to transmitter, the theorem is still valid. The encoder can then change the code word suffixes depending on which $\mathbf{y}_1$ is received, but (2.5) is valid independent of the choice of the set $\{\mathbf{x}_{m,2}\}$. Finally the theorem can be extended to the case where two independent channels are available and $\mathbf{x}_{m,1}$ is sent over one channel and $\mathbf{x}_{m,2}$ is sent over the other channel.

## III. ERROR PROBABILITY FOR TWO CODE WORDS

In this section we shall derive both upper and lower bounds to the probability of decoding error for a block code with two code words of length $N$. Surprisingly enough, the results are fundamental to both Sections IV and V.

Let $P_m(\mathbf{y})$, $m = 1, 2$, be the probability of receiving sequence $\mathbf{y}$ when message $m$ is transmitted. If $Y_m$ is the set of sequences decoded into message $m$, then from (1.2), the probability of decoding error when message $m$ is transmitted is

$$P_{e,m} = \sum_{\mathbf{y} \in Y_m{}^c} P_m(\mathbf{y}); \qquad m = 1, 2 \tag{3.1}$$

For initial motivation, suppose that the decoder adopts a maximum likelihood decision rule: decode $\mathbf{y}$ into message 1 if $P_1(\mathbf{y}) > P_2(\mathbf{y})$ and decode into message 2 otherwise. Under these circumstances $P_m(\mathbf{y})$ in (3.1) is equal to $\min_{m'=1,2} P_{m'}(\mathbf{y})$. Summing (3.1) over $m$, we then get

$$P_{e,1} + P_{e,2} = \sum_{\mathbf{y}} \min_{m=1,2} P_m(\mathbf{y}) \tag{3.2}$$

For any $s$ in the interval $0 < s < 1$, a simple bound on $\min P_m(\mathbf{y})$ is given by

$$\min_{m=1,2} P_m(\mathbf{y}) \leqq P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s \leqq \max_{m=1,2} P_m(\mathbf{y}) \tag{3.3}$$

Thus,

$$P_{e,1} + P_{e,2} \leqq \sum_{\mathbf{y}} P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s; \qquad 0 < s < 1 \tag{3.4}$$

We shall see later that when the right hand side of (3.4) is minimized over $s$, the bound is quite tight despite its apparent simplicity.

The logarithm of the right side of (3.4) is a fundamental quantity in most of the remainder of this paper; we denote it by

$$\mu(s) \triangleq \ln \sum_{\mathbf{y}} P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s; \qquad 0 < s < 1 \tag{3.5}$$

It is convenient to extend this definition to cover $s = 0$ and $s = 1$.

$$\mu(0) \triangleq \lim_{s \to 0^+} \mu(s); \qquad \mu(1) \triangleq \lim_{s \to 1^-} \mu(s) \tag{3.6}$$

Then we can rewrite (3.4), minimized over $s$, as

$$P_{e,1} + P_{e,2} \leqq \min_{0 \leqq s \leqq 1} \exp \mu(s) \tag{3.7}$$

Some typical modes of behavior of $\mu(s)$ are shown in Fig. 5. The block length in these figures is one and the first code word is the input letter 1 and the second is the input letter 2. It is shown later that $\mu(s)$ is always nonpositive and convex $\cup$.

We next show that when the block length is greater than one, $\mu(s)$ can be written as a sum over the individual letters in the block. Let the code words be denoted by $\mathbf{x}_m = (k_{m,1}, \cdots, k_{m,N})$, $m = 1, 2$, and let the received sequence be $\mathbf{y} = (j_1, \cdots, j_N)$. Then, using (1.1), we have $P_m(\mathbf{y}) = \prod_n P(j_n \mid k_{m,n})$, and $\mu(s)$ becomes

$$\mu(s) = \ln \sum_{j_1=1}^{J} \cdots \sum_{j_N=1}^{J} \prod_{n=1}^{N} P(j_n \mid k_{1,n})^{1-s} P(j_n \mid k_{2,n})^s \tag{3.8}$$

$$\begin{aligned} \mu(s) = \ln \sum_{j_1=1}^{J} P(j_1 \mid k_{1,1})^{1-s} P(j_1 \mid k_{2,1})^s \sum_{j_2=1}^{J} P(j_2 \mid k_{1,2})^{1-s} \\ \cdot P(j_2 \mid k_{2,2})^s \cdots \sum_{j_N=1}^{J} P(j_N \mid k_{1,N})^{1-s} P(j_N \mid k_{2,N})^s \end{aligned} \tag{3.9}$$

$$\mu(s) = \sum_{n=1}^{N} \mu_n(s); \qquad \mu_n(s) = \ln \sum_{j=1}^{J} P(j \mid k_{1,n})^{1-s} P(j \mid k_{2,n})^s \tag{3.10}$$

We now generalize the bound in (3.7) in two directions. First we want both upper and lower bounds on $P_{e,1}$ and $P_{e,2}$. Second, for reasons that will be clear in Section IV, we want to allow ourselves the flexibility of making $P_{e,1}$ very much larger than $P_{e,2}$ or vice versa. The following theorem achieves both of these objectives.

THEOREM 5. *Let $P_1(\mathbf{y})$ and $P_2(\mathbf{y})$ be two probability assignments on a*

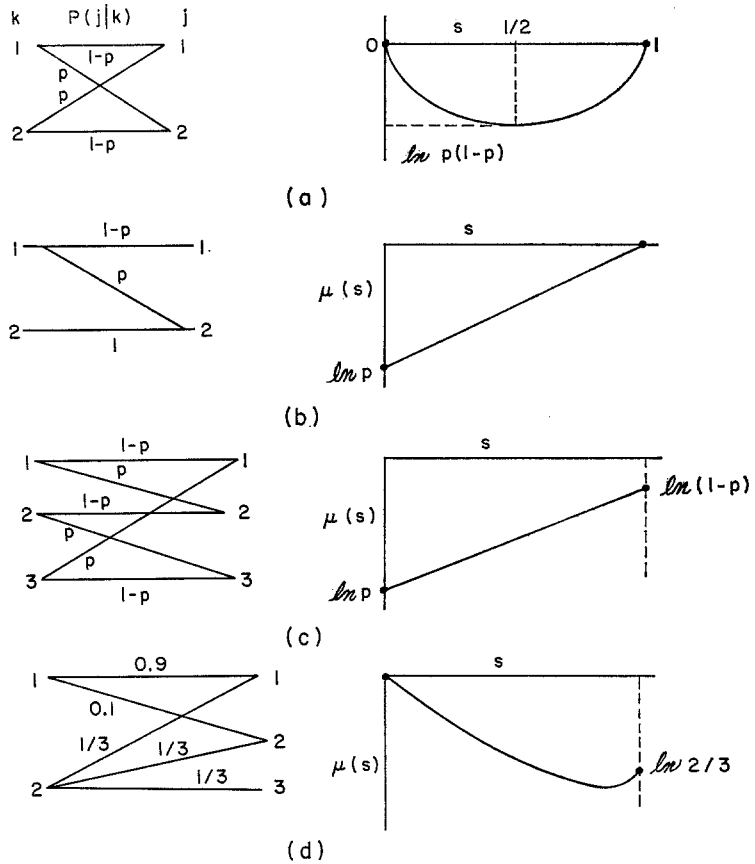


FIG. 5. The functions $\mu(s) = \ln \sum_j P(j \mid 1)^{1-s} P(j \mid 2)^s$ for several channels.

*discrete set of sequences, let* $Y_1$ *and* $Y_2$ *be disjoint decision regions for these sequences, let* $P_{e,1}$ *and* $P_{e,2}$ *be given by* (3.1) *and assume that* $P_1(\mathbf{y})P_2(\mathbf{y}) \neq 0$ *for at least one sequence* $\mathbf{y}$. *Then, for any* $s$, $0 < s < 1$, *either*

$$P_{e,1} > \tfrac{1}{4} \exp\left[\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}\right] \tag{3.11}$$

*or*

$$P_{e,2} > \tfrac{1}{4} \exp\left[\mu(s) + (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}\right] \tag{3.12}$$

*Furthermore, for an appropriate choice of* $Y_1$, $Y_2$,

$$P_{e,1} \leqq \exp [\mu(s) - s\mu'(s)] \qquad \textit{and} \tag{3.13}$$

$$P_{e,2} \leqq \exp [\mu(s) + (1 - s)\mu'(s)] \tag{3.14}$$

*Finally* $\mu(s)$ *is nonpositive and convex* $\cup$ *for* $0 < s < 1$. *The convexity is strict unless* $P_1(\mathbf{y})/P_2(\mathbf{y})$ *is constant over all* $\mathbf{y}$ *for which* $P_1(\mathbf{y})P_2(\mathbf{y}) \neq 0$. *Also* $\mu(s)$ *is strictly negative for* $0 < s < 1$ *unless* $P_1(\mathbf{y}) = P_2(\mathbf{y})$ *for all* $\mathbf{y}$.

*Remarks:* The probabilities $P_1(\mathbf{y})$ and $P_2(\mathbf{y})$ do not have to correspond to two code words and in Section IV the theorem will be used where $P_2(\mathbf{y})$ does not correspond to a code word. For interpretation, however, we shall consider only the problem of two code words on a memoryless channel, in which case (3.10) is valid. Taking the derivatives of (3.10), we have

$$\mu'(s) = \sum_{n=1}^{N} \mu_n'(s); \qquad \mu''(s) = \sum_{n=1}^{N} \mu_n''(s) \tag{3.15}$$

Therefore, for any $s$, $0 < s < 1$, the first part of the theorem states that either

$$P_{e,1} > \tfrac{1}{4} \exp\left\{\sum_{n=1}^{N} [\mu_n(s) - s\mu_n'(s)] - s\sqrt{\sum_n 2\mu_n''(s)}\right\} \tag{3.16}$$

or

$$P_{e,2} > \tfrac{1}{4} \exp\left\{\sum_{n=1}^{N} [\mu_n(s) + (1 - s)\mu_n'(s)] - (1 - s) \cdot \sqrt{\sum_n \mu_n''(s)}\right\} \tag{3.17}$$

We see from this that in some sense the terms involving $\mu(s)$ and $\mu'(s)$ are proportional to the block length $N$ and that the term involving $\sqrt{\mu''(s)}$ is proportional to $\sqrt{N}$. It follows that for large $N$ we should focus our attention primarily on $\mu(s)$ and $\mu'(s)$.

Figure 6 gives a graphical interpretation of the terms $\mu(s) - \mu'(s)$ and $\mu(s) + (1 - s)\mu'(s)$. It is seen that they are the endpoints, at 0 and 1, of the tangent at $s$ to the curve $\mu(s)$. As $s$ increases, the tangent see-saws around, decreasing $\mu(s) - s\mu'(s)$ and increasing $\mu(s) + (1 - s)\mu'(s)$. In the special case where $\mu(s)$ is a straight line, of course, this see-sawing does not occur and $\mu(s) - s\mu'(s)$ and $\mu(s) + (1 - s)\mu'(s)$ do not vary with $s$.

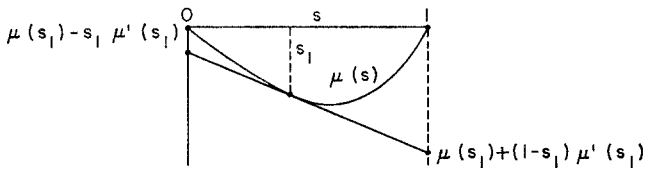


FIG. 6. Geometric interpretation of the exponents $\mu(s) - s\mu'(s)$ and $\mu(s) + (1 - s)\mu'(s)$.

Since $\mu(s)$ is convex $\cup$ over $0 < s < 1$, any tangent to $\mu$ in this range will lie on or beneath $\mu$. Furthermore, since $\mu(s) \leqq 0$ in this range, we have in general, for $0 < s < 1$,

$$\mu(s) - s\mu'(s) \leqq 0 \tag{3.18}$$

$$\mu(s) + (1 - s)\mu'(s) \leqq 0 \tag{3.19}$$

A particularly important special case of the theorem is that in which $s$ is chosen to minimize $\mu(s)$. In that case we get the following corollary.

COROLLARY. *Let* $s^*$ *minimize* $\mu(s)$ *over* $0 \leqq s \leqq 1$. *Then either*

$$P_{e,1} \geqq \tfrac{1}{4} \exp\left[\mu(s^*) - s^*\sqrt{2\mu''(s^*)}\right] \tag{3.20}$$

*or*

$$P_{e,2} \geqq \tfrac{1}{4} \exp\left[\mu(s^*) - (1 - s^*)\sqrt{2\mu''(s^*)}\right] \tag{3.21}$$

*where if* $s^* = 0$ *or* 1, $\mu''(s^*)$ *is the limit of* $\mu''(s)$ *from the interior of the interval.*

*Proof of Corollary:* If $s^*$ is within the interval $0 < s^* < 1$, then $\mu'(s^*) = 0$ and (3.20) and (3.21) follow immediately from (3.11) and (3.12). If $s^* = 0$, then $\mu'(0^+) \geqq 0$, and

$$\begin{aligned} \lim_{s\to 0^+} \mu(s) - s\mu'(s) &= \mu(0^+) = \mu(s^*) \\ \lim_{s\to 0^+} \mu(s) + (1 - s)\mu'(s) &\geqq \mu(0^+) = \mu(s^*) \end{aligned} \tag{3.22}$$

Likewise if $s^* = 1$, *then* $\mu'(1^-) \leqq 0$, and

$$\begin{aligned} \lim_{s\to 1^-} \mu(s) - s\mu'(s) &\geqq \mu(1^-) = \mu(s^*) \\ \lim_{s\to 1^-} \mu(s) + (1 - s)\mu'(s) &= \mu(1^-) = \mu(s^*) \end{aligned} \tag{3.23}$$

Substituting these relations into (3.11) and (3.12) completes the proof.

Notice that the exponent $\mu(s^*)$ appearing in (3.20) and (3.21) is the same as the exponent in the upper bound to $P_{e,1} + P_{e,2}$ of (3.7).

*Proof of Theorem 5:* The sum over $\mathbf{y}$ in $\mu(s)$ as given by (3.5) can either be considered to be over all output sequences $\mathbf{y}$ or over only those sequences in the overlap region where $P_1(\mathbf{y})$ and $P_2(\mathbf{y})$ are both nonzero. For the remainder of the proof, we consider all sums over $\mathbf{y}$ to be over only the overlap region.

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

$$\mu'(s) = \left\{ \sum_{\mathbf{y}} \frac{P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s}{\sum_{\mathbf{y}'} P_1(\mathbf{y}')^{1-s} P_2(\mathbf{y}')^s} \ln \frac{P_2(\mathbf{y})}{P_1(\mathbf{y})} \right. \tag{3.24}$$

$$\mu''(s) = \left\{ \sum_{\mathbf{y}} \frac{P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s}{\sum_{\mathbf{y}'} P_1(\mathbf{y}')^{1-s} P_2(\mathbf{y}')^s} \left[ \ln \frac{P_2(\mathbf{y})}{P_1(\mathbf{y})} \right]^2 \right\} - [\mu'(s)]^2 \tag{3.25}$$

Let $D(\mathbf{y})$ be the log likelihood ratio,

$$D(\mathbf{y}) = \ln \frac{P_2(\mathbf{y})}{P_1(\mathbf{y})} \tag{3.26}$$

and for $0 < s < 1$, define

$$Q_s(\mathbf{y}) = \frac{P_1(\mathbf{y})^{1-s} P_2(\mathbf{y})^s}{\sum_{\mathbf{y}'} P_1(\mathbf{y}')^{1-s} P_2(\mathbf{y}')^s} \tag{3.27}$$

It will be seen later that $Q_s(\mathbf{y})$ is large for those $\mathbf{y}$ that are likely to cause errors; thus this probability assignment allows us to focus our attention on the region of interest.

If we consider $D(\mathbf{y})$ to be a random variable with probability assignment $Q_s(\mathbf{y})$, then we see from (3.24) and (3.25) that $\mu'(s)$ and $\mu''(s)$ are the mean and variance of $D(\mathbf{y})$ respectively. Since $\mu''(s)$ is a variance, it is nonnegative and therefore $\mu(s)$ is convex $\cup$. It can also be seen from this that $\mu(s)$ will be strictly convex $\cup$ unless $P_2(\mathbf{y})/P_1(\mathbf{y})$ is a constant for all $\mathbf{y}$ in the overlap region. Since $\mu(0)$ and $\mu(1)$ are nonpositive (see (3.5) and (3.6)), it follows from convexity that $\mu$ is nonpositive for all $s$, $0 \leqq s \leqq 1$. Furthermore, for $\mu(s)$ to be 0 at any point within the interval $(0, 1)$ it is necessary for $\mu(0)$, $\mu(1)$, and $\mu''(s)$ all to be zero. It is easy to see that this can happen only if $P_1(\mathbf{y}) = P_2(\mathbf{y})$ for all $\mathbf{y}$.

It can be verified easily by substituting (3.26) and (3.5) into (3.27) that

$$P_1(\mathbf{y}) = \{\exp [\mu(s) - sD(\mathbf{y})]\} Q_s(\mathbf{y}) \tag{3.28}$$

$$P_2(\mathbf{y}) = \{\exp[\mu(s) + (1-s)D(\mathbf{y})]\}Q_s(\mathbf{y}) \tag{3.29}$$

We shall now establish the second part of the theorem, (3.13) and (3.14). For a given $s$, define the decision region $Y_1$ to be

$$Y_1 = \{\mathbf{y}: D(\mathbf{y}) < \mu'(s)\} \tag{3.30}$$

Then for $\mathbf{y} \in Y_1^c$, we have $-sD(\mathbf{y}) \leqq -s\mu'(s)$, and (3.28) is bounded by

$$P_1(\mathbf{y}) \leqq \{\exp[\mu(s) - s\mu'(s)]\}Q_s(\mathbf{y}); \qquad \mathbf{y} \in Y_1^c \tag{3.31}$$

Substituting (3.31) into (3.1), we have

$$P_{e,1} \leqq \{\exp[\mu(s) - s\mu'(s)]\} \sum_{\mathbf{y} \in Y_1^c} Q_s(\mathbf{y}) \tag{3.32}$$

Equation (3.13) follows upon upper bounding the sum of probabilities in (3.32) by 1. Equation (3.14) follows in the same way upon recognizing that $(1-s)D(\mathbf{y}) \leqq (1-s)\mu'(s)$ for $\mathbf{y} \in Y_2^c$.

We now turn to the proof of the first part of the theorem. Define $Y_s$ as the set of sequences for which $D(\mathbf{y})$ is within $\sqrt{2}$ standard deviations of its mean according to $Q_s(\mathbf{y})$.

$$Y_s = \{\mathbf{y}: | D(\mathbf{y}) - \mu'(s) | \leqq \sqrt{2\mu''(s)}\} \tag{3.33}$$

From the Chebychev inequality,

$$\sum_{\mathbf{y} \in Y_s} Q_s(\mathbf{y}) > \tfrac{1}{2} \tag{3.34}$$

We now lower bound $P_{e,1}$ and $P_{e,2}$ by considering only those $\mathbf{y}$ in the set $Y_s$. This is motivated by the fact that for the decision rule (3.30), most of the errors presumably occur when $| D(\mathbf{y}) - \mu'(s)|$ is small.

$$P_{e,1} = \sum_{\mathbf{y} \in Y_1^c} P_1(\mathbf{y}) \geqq \sum_{\mathbf{y} \in Y_1^c \cap Y_s} P_1(\mathbf{y}) \tag{3.35}$$

$$P_{e,2} = \sum_{\mathbf{y} \in Y_2^c} P_2(\mathbf{y}) \geqq \sum_{\mathbf{y} \in Y_2^c \cap Y_s} P_2(\mathbf{y}) \tag{3.36}$$

For $\mathbf{y} \in Y_s$, (3.33) gives us

$$\mu'(s) - \sqrt{2\mu''(s)} \leqq D(\mathbf{y}) \leqq \mu'(s) + \sqrt{2\mu''(s)} \tag{3.37}$$

Thus, for $\mathbf{y} \in Y_s$, (3.28) and (3.29) are bounded by

$$P_1(\mathbf{y}) \geqq \{\exp[\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}]\}Q_s(\mathbf{y}) \tag{3.38}$$

$$P_2(\mathbf{y}) \geqq \{\exp[\mu(s) - (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}]\} \cdot Q_s(\mathbf{y}) \tag{3.39}$$

Substituting (3.38) into (3.35) and (3.39) into (3.36) leaves only $Q_s(\mathbf{y})$ under the summation signs.

$$P_{e,1} \geqq \{\exp[\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}]\} \sum_{\mathbf{y} \in Y_1^c \cap Y_s} Q_s(\mathbf{y}) \tag{3.40}$$

$$P_{e,2} \geqq \{\exp[\mu(s) + (1-s)\mu'(s) - (1-s)\sqrt{2\mu''(s)}]\} \cdot \sum_{\mathbf{y} \in Y_2^c \cap Y_s} Q_s(\mathbf{y}) \tag{3.41}$$

Since $Y_1$ and $Y_2$ are disjoint, (3.34) yields

$$\sum_{\mathbf{y} \in Y_1^c \cap Y_s} Q_s(\mathbf{y}) + \sum_{\mathbf{y} \in Y_2^c \cap Y_s} Q_s(\mathbf{y}) > \tfrac{1}{2} \tag{3.42}$$

Thus, either

$$\sum_{\mathbf{y} \in Y_1^c \cap Y_s} Q_s(\mathbf{y}) > \tfrac{1}{4} \tag{3.43}$$

or

$$\sum_{\mathbf{y} \in Y_2^c \cap Y_s} Q_s(\mathbf{y}) > \tfrac{1}{4} \tag{3.44}$$

Substituting these inequalities into (3.40) and (3.41) completes the proof of the theorem.

There are a number of other approaches that could have been taken to prove theorems essentially equivalent to Theorem 3. The theorem treats a simple statistical decision theory problem with 2 hypotheses. According to the Neyman-Pearson (1928) theorem, we can minimize $P_{e,1}$ for a given value of $P_{e,2}$ by letting $Y_1$ be the set of $\mathbf{y}$ for which $D(\mathbf{y})$ is less than a constant chosen to give $P_{e,2}$ its given value. Then $P_{e,1}$ is the probability according to $P_1(\mathbf{y})$ that $D(\mathbf{y})$, which is the sum of $N$ independent random variables, is greater than or equal to that constant. Likewise, $P_{e,2}$ is the probability according to $P_2(\mathbf{y})$ that $D(\mathbf{y})$ is less than the constant. A number of estimates and bounds on the probability that a sum of independent random variables will be far from the mean are given by Feller (1943), Chernoff (1952), Chapter 8 of Fano (1961), and Gallager (1965b). The particular theorem chosen here was selected primarily for the simplicity of the result and for its generality. Observe that Theorem 5 is applicable whenever $\mu(s)$ and its first two derivatives exist. For example $\mathbf{y}$ may be a sequence of real numbers and $P_1(\mathbf{y})$ and $P_2(\mathbf{y})$ may be replaced with probability densities.

## IV. THE SPHERE PACKING BOUND

Let $\mathbf{x}_1, \mathbf{x}_2, \cdots, \mathbf{x}_M$ be a set of $M$ code words each of length $N$ for use on a discrete memoryless channel with transition probabilities $P(j \mid k)$. Assume a list decoding scheme in which for each received sequence $\mathbf{y}$, the decoder produces a list of at most $L$ integers from 1 to $M$. If $Y_m$ is the set of output sequences $\mathbf{y}$ for which message $m$ is on the decoding list, then, as in (1.2), the probability of list decoding error when message $m$ is sent is

$$P_{e,m} = \sum_{\mathbf{y} \in Y_m{}^c} \Pr(\mathbf{y} \mid \mathbf{x}_m) \tag{4.1}$$

Let $P_{e,\max}$ be the maximum over $m$ of $P_{e,m}$ for the code and list decoding scheme under consideration. In this section we first find a lower bound on $P_{e,\max}$ for a special class of codes called fixed composition codes. We then generalize the results to arbitrary codes, and prove Theorem 2 of the introduction.

For any given $m$, $P_{e,m}$ can generally be reduced by enlarging the size of the decoding set $Y_{m'}$ this will decrease the size of $Y_{m'}$, for some $m' \neq m$, however, and thus generally increase $P_{e,m'}$. In order to keep some control over the size of $Y_m$ without specifically considering the other code words, we define an arbitrary product probability measure on the output sequences $\mathbf{y} = (j_1, \cdots, j_N)$,

$$f_N(\mathbf{y}) = \prod_{n=1}^{N} f(j_n) \tag{4.2}$$

where $\mathbf{f} = \{f(1), \cdots, f(J)\}$ is an arbitrary probability assignment on the output letters 1 to $J$. The size of $Y_m$ is now defined as

$$F(Y_m) = \sum_{\mathbf{y} \in Y_m} f_N(\mathbf{y}) \tag{4.3}$$

Theorem 5 can be used to relate $P_{e,m}$ and $F(Y_m)$ if we let $\Pr(\mathbf{y} \mid \mathbf{x}_m)$ correspond to $P_1(\mathbf{y})$ in the theorem and let $f_N(\mathbf{y})$ correspond to $P_2(\mathbf{y})$. The function $\mu(s)$ of Theorem 5 corresponding to $\Pr(\mathbf{y} \mid \mathbf{x}_m)$ and $f_N(\mathbf{y})$ is given by

$$\mu(s) = \ln \sum_{\mathbf{y}} \Pr(\mathbf{y} \mid \mathbf{x}_m)^{1-s} f_N(\mathbf{y})^s \tag{4.4}$$

Assume that $\Pr(\mathbf{y}/\mathbf{x}_m) f_N(\mathbf{y}) \neq 0$ for at least one $\mathbf{y}$. Theorem 5 then states that for each $s$, $0 < s < 1$, either

$$P_{e,m} > \tfrac{1}{4} \exp[\mu(s) - s\mu'(s) - s\sqrt{2\mu''(s)}] \tag{4.5}$$

or

$$F(Y_m) > \tfrac{1}{4} \exp [\mu(s) + (1 - s)\, \mu'(s) - (1 - s) \sqrt{2\mu''(s)}] \quad (4.6)$$

Since $f_N(\mathbf{y}) = \prod_n f(j_n)$, $\mu(s)$ can be broken up into a sum of terms as in (3.10). If $\mathbf{x}_m = (k_{m,1}, \cdots, k_{m,N})$, we have

$$\mu(s) = \sum_{n=1}^{N} \mu_{k_{m,n}}(s, \mathbf{f}) \quad (4.7)$$

$$\mu_k(s, \mathbf{f}) = \ln \sum_j P(j/k)^{1-s} f(j)^s \quad (4.8)$$

The function $\mu(s)$ depends on $\mathbf{x}_m$ only through the number of appearances of each alphabet letter in $\mathbf{x}_m$. Let

$$q_k(m) = \frac{\text{Number of times input letter } k \text{ appears in } \mathbf{x}_m}{N} \quad (4.9)$$

The vector $\mathbf{q}(m) = (q_1(m), \cdots, q_K(m))$ is called the composition of the $m$th code word. In terms of $\mathbf{q}(m)$, $\mu(s)$ becomes

$$\mu(s) = N \sum_{k=1}^{K} q_k(m) \mu_k(s, \mathbf{f}) \quad (4.10)$$

Let us restrict our attention temporarily to codes in which all code words have the same composition. Then the $m$ can be dropped from $q_k(m)$ in (4.10), and (4.5) and (4.6) become: for each $s$, $0 < s < 1$, either

$$P_{e,m} > \tfrac{1}{4} \exp N \left\{ \sum_k q_k [\mu_k(s, \mathbf{f}) - s\mu_k'(s, \mathbf{f})] - \frac{s}{\sqrt{N}} \sqrt{2 \sum_k q_k \mu_k''(s, \mathbf{f})} \right\} \quad (4.11)$$

or

$$F(Y_m) > \tfrac{1}{4} \exp N \left\{ \sum_k q_k [\mu_k(s, \mathbf{f}) + (1 - s) \mu_k'(s, \mathbf{f})] - \frac{(1 - s)}{\sqrt{N}} \sqrt{2 \sum_k q_k \mu_k''(s, \mathbf{f})} \right\} \quad (4.12)$$

The square root terms in (4.11) and (4.12) turn out to be unimportant for large $N$. Thus we simplify the expressions by the following loose but general bound on $\mu_k''$ (see appendix).

$$s\sqrt{\mu_k''(s, \mathbf{f})} \leqq \ln \frac{e}{\sqrt{P_{\min}}} \tag{4.13}$$

$P_{\min}$ is the smallest nonzero transition probability on the channel.

We can now relate $F(Y_m)$ to the number of code words $M$ and the list size $L$ by observing that

$$\sum_{m=1}^{M} F(Y_m) = \sum_{m=1}^{M} \sum_{\mathbf{y} \in Y_m} f_N(\mathbf{y}) \leqq L \tag{4.14}$$

Equation (4.14) follows from the facts that each $\mathbf{y}$ appears in at most $L$ decoding subsets and that $\sum_{\mathbf{y}} f_N(\mathbf{y}) = 1$. As a consequence of (4.14), there must be some $m$ for which

$$F(Y_m) \leqq L/M \tag{4.15}$$

For this $m$, we can substitute (4.13) and (4.15) into (4.11) and (4.12). Bringing the factors of $\frac{1}{4}$ inside the exponents and upper bounding $P_{e,m}$ by $P_{e,\max}$, (4.11) and (4.12) become: either

$$P_{e,\max} > \exp N \left\{ \sum_{k=1}^{K} q_k[\mu_k(s, \mathbf{f}) - s\mu_k'(s, \mathbf{f})] - \sqrt{\frac{2}{N}} \ln \frac{e}{\sqrt{P_{\min}}} - \frac{\ln 4}{N} \right\} \tag{4.16}$$

or

$$\frac{L}{M} > \exp N \left\{ \sum_{k=1}^{K} q_k[\mu_k(s, \mathbf{f}) + (1 - s)\mu_k'(s, \mathbf{f})] - \frac{1 - s}{s} \sqrt{\frac{2}{N}} \ln \frac{e}{\sqrt{P_{\min}}} - \frac{\ln 4}{N} \right\} \tag{4.17}$$

Equations (4.16) and (4.17) provide a parametric lower bound on $P_{e,\max}$ for a given $L/M$ in terms of the parameter $s$ in the same way that Theorem 5 provided a parametric lower bound on $P_{e,1}$ for a given $P_{e,2}$. The bound is valid for any fixed composition code of composition $\mathbf{q}$ with $M$ code words of length $N$ and for any list decoding scheme with lists of size $L$.

The reason for calling this a sphere packing bound is somewhat historical, but also adds some insight into what we have done. From the discussion following Theorem 5, we see that $P_{e,m}$ can be minimized for a decoding subset of given size by picking the set $Y_m$ to be those $\mathbf{y}$ for which $\ln [f_N(\mathbf{y})/\Pr(\mathbf{y} \mid \mathbf{x}_m)]$ is less than a constant. If we think of

$\ln [f_N(\mathbf{y})/\Pr(\mathbf{y} \mid \mathbf{x}_m)]$ as a generalized type of distance from $\mathbf{x}_m$ to $\mathbf{y}$, then we can think of the $Y_m$ that minimizes $P_{e,m}$ as being a sphere around $\mathbf{x}_m$. Thus our bound on $P_{e,\max}$ in terms of $M$ would be a very tight bound if we could pick the $Y_m$ as a set of spheres, each sphere around one code word, with spheres packed into the space of output sequences.

The bound of (4.16) and (4.17) is a function of the arbitrary probability assignment $\mathbf{f}$. The straightforward approach now would be to find that $\mathbf{f}$ which yields the tightest bound on $P_{e,\max}$, i.e., that *maximizes* the lower bound for a given composition. We could then look for the best composition, i.e., the $\mathbf{q}$ that *minimizes* the lower bound on $P_{e,\max}$. Such a procedure turns out to be both tedious and unenlightening. We shall instead simply state the resulting $\mathbf{f}$ and $\mathbf{q}$ as functions of the parameter $s$ and then show that this choice gives us the bound of Theorem 2.

For a given $s$, $0 < s < 1$, let $\mathbf{q}_s = (q_{1,s}, \cdots, q_{K,s})$ satisfy the equations

$$\sum_j P(j \mid k)^{1-s} \alpha_{j,s}^{s/(1-s)} \geqq \sum_j \alpha_{j,s}^{1/(1-s)}; \qquad \text{all } k \tag{4.18}$$

where

$$\alpha_{j,s} = \sum_{k=1}^{K} q_{k,s} P(j \mid k)^{1-s} \tag{4.19}$$

Let $\mathbf{f}_s = (f_s(1), \cdots, f_s(J))$ be given by

$$f_s(j) = \frac{\alpha_{j,s}^{1/(1-s)}}{\sum_{j'=1}^{J} \alpha_{j',s}^{1/(1-s)}} \tag{4.20}$$

This is a rather formidable looking set of equations, but the solutions have some remarkable properties. If we set $\rho = s/(1-s)$, (4.18) and (4.19) are identical to the necessary and sufficient conditions (1.14) and (1.15) on $\mathbf{q}$ to maximize the function $E_0(\rho, \mathbf{q})$ discussed in Section I. Thus (4.18) is satisfied with equality for those $k$ with $q_{k,s} > 0$. Since $E_0(\rho, \mathbf{q})$ must have a maximum over the probability vectors $\mathbf{q}$, (4.18) and (4.19) must have a solution (though it need not be unique).

The fact that $\mathbf{f}$ is chosen here as a function of $s$ in no way changes the validity of the lower bound to $P_{e,\max}$ given by (4.16) and (4.17). We must remember, however, that $\mu_k'(s, \mathbf{f}_s)$ is the partial derivative of $\mu_k$

with respect to $s$ holding $\mathbf{f}_s$ fixed. The condition that for each $k, f(j)P(j \mid k) \neq 0$ for some $j$ is clearly met by $\mathbf{f}_s$, since the left side of (4.18) must be strictly positive.

Next we show that $\mathbf{f}_s$ has the property that $\mu_k(s, \mathbf{f}_s)$ is independent of $k$ for those inputs with $q_{k,s} \neq 0$. Substituting (4.20) into the expression (4.8) for $\mu_k$, we have

$$\mu_k(s, \mathbf{f}_s) = \ln \sum_{j=1}^{J} P(j \mid k)^{1-s} \alpha_{j,s}^{s/(1-s)} - s \ln \sum_{j=1}^{J} \alpha_{j,s}^{1/(1-s)} \quad (4.21)$$

Using (4.18) in (4.21),

$$\mu_k(s, \mathbf{f}_s) \geqq (1 - s) \ln \sum_{j=1}^{J} \alpha_{j,s}^{1/(1-s}$$

with equality if $q_{k,s} \neq 0$. Finally, using (4.19) for $\alpha_{j,s}$, we have the expression for $E_0(\rho)$ in (1.8) and (1.9). Thus

$$\mu_k(s, \mathbf{f}_s) \geqq -(1 - s)E_0\left(\frac{s}{1 - s}\right); \qquad \text{equality if } q_{k,s} \neq 0 \quad (4.22)$$

One final property of $\mathbf{q}_s$ and $\mathbf{f}_s$, which we shall not need but which gives some insight into why $\mathbf{f}_s$ yields the tightest bound on $P_{e,\max}$ for the "best" composition $\mathbf{q}_s$, is that $\mathbf{q}_s$, $\mathbf{f}_s$ yields a min-max point for the function $\sum_k q_k \mu_k(s, \mathbf{f})$. That is, for all $\mathbf{q}$, $\mathbf{f}$,

$$\sum_k q_{k,s}\mu_k(s, \mathbf{f}) \leqq \sum_k q_{k,s}\mu_k(s, \mathbf{f}_s) \leqq \sum_k q_k \mu_k(s, \mathbf{f}_s) \quad (4.23)$$

This relation is established in the appendix.

We can now state a theorem that is equivalent to Theorem 2 in the introduction, with the exception that the theorem here applies only to fixed composition codes.

THEOREM 6. *Let $P(j \mid k)$ be the transition probabilities for a discrete memoryless channel and let a fixed composition code for the channel have $M$ code words of length $N$ with a list decoding scheme of list size $L$. Then at least one code word will have a probability of list decoding error bounded by*

$$P_{e,\max} \geqq \exp - N\left\{E_{sp}\left(R - \frac{\ln 4}{N} - \epsilon\right) + \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}\right\} \quad (4.24)$$

*where* $R = (1/N) \ln (M/L)$, *the function* $E_{sp}$ *is given by* (1.7), *and* $\epsilon$ *is an arbitrarily small positive number.*

*Proof*: We shall first express the parametric lower bound on $P_{e,\max}$ of (4.16) and (4.17) in a more convenient way. Define $R(s, \mathbf{q})$ as minus the quantity in braces in (4.17), using $\mathbf{f}_s$ for $\mathbf{f}$.

$$R(s, \mathbf{q}) = \sum_k - q_k[\mu_k(s, \mathbf{f}_s) + (1 - s)\mu_k'(s, \mathbf{f}_s)] + \frac{1 - s}{s} \sqrt{\frac{2}{N}} \ln \frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N} \tag{4.25}$$

Then (4.17) can be rewritten

$$R = \frac{\ln M/L}{N} < R(s, \mathbf{q}) \tag{4.26}$$

Also we can use (4.25) to eliminate the $\mu_k'$ term in (4.16), getting

$$P_{e,\max} > \exp N \left\{ \sum_k q_k \left(1 + \frac{s}{1 - s}\right) \mu_k(s, \mathbf{f}_s) + \frac{s}{1 - s} R(s, \mathbf{q}) - \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} - \left(1 + \frac{s}{1 - s}\right) \frac{\ln 4}{N} \right\} \tag{4.27}$$

Thus, for every $s$, $0 < s < 1$, either (4.26) or (4.27) is satisfied.

We now consider two separate cases

(a) $$R = R(s, \mathbf{q}) \quad \text{for some } s, \quad 0 < s < 1 \tag{4.28}$$

(b) $$R < R(s, \mathbf{q}) \quad \text{for all } s, \quad 0 < s < 1 \tag{4.29}$$

It is shown in the appendix that $R(s, \mathbf{q})$ is a continuous function of $s$ for $0 < s < 1$, and it can be seen from the term containing $(1 - s)/s$ in (4.25) that $\lim_{s \to 0} R(s, \mathbf{q}) = \infty$. Thus either (a) or (b) above must be satisfied. If (a) is satisfied for some $s$, then (4.26) is unsatisfied and (4.27) must be satisfied for that $s$; substituting (4.22) and (4.28) into (4.27), we have

$$P_{e,\max} > \exp N \left\{ -E_0 \left(\frac{s}{1 - s}\right) + \frac{s}{1 - s} \left(R - \frac{\ln 4}{N}\right) - \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} - \frac{\ln 4}{N} \right\} \tag{4.30}$$

Using $\rho$ for $s/(1 - s)$ and further lower bounding by taking the lowest

upper bound of the negative exponent over $\rho$, we have

$$P_{e,\max} > \exp - N\left\{\underset{\rho\geqq 0}{\text{L.U.B.}}\left[E_0(\rho) - \rho\left(R - \frac{\ln 4}{N}\right)\right] + \sqrt{\frac{8}{N}}\ln\frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}\right\} \tag{4.31}$$

$$> \exp - N\left\{\underset{\rho\geqq 0}{\text{L.U.B.}}\left[E_0(\rho) - \rho\left(R - \frac{\ln 4}{N} - \epsilon\right)\right] + \sqrt{\frac{8}{N}}\ln\frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}\right\} \tag{4.32}$$

Using the definition of $E_{sp}$ in (1.7), this is equivalent to (4.24) and proves the theorem for case (a).

Next we show that for case (b), (4.24) reduces to $P_{e,\max} \geqq 0$ which is trivially true. From (3.18),

$$\mu_k(s, \mathbf{f}_s) - s\mu_k'(s, \mathbf{f}_s) \leqq 0; \quad -\mu_k'(s, \mathbf{f}_s) \leqq \frac{-\mu_k(s, \mathbf{f}_s)}{s} \tag{4.33}$$

Substituting (4.33) into (4.25), we obtain for all $s$, $0 < s < 1$,

$$R < R(s, \mathbf{q}) \leqq -\sum_{k=1}^{K} q_k\left(1 + \frac{1-s}{s}\right)\mu_k(s, \mathbf{f}_s) + \frac{1-s}{s}\sqrt{\frac{2}{N}}\ln\frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}$$

Using (4.22) again and letting $\rho = s/(1-s)$, this becomes

$$R < \frac{E_0(\rho)}{\rho} + \frac{1}{\rho}\sqrt{\frac{2}{N}}\ln\frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}; \qquad \text{all } \rho > 0 \tag{4.34}$$

Using (1.7) and (4.34), we have

$$E_{sp}\left(R - \frac{\ln 4}{N} - \epsilon\right) = \underset{\rho\geqq 0}{\text{L.U.B.}}\left[E_0(\rho) - \rho\left(R - \frac{\ln 4}{N} - \epsilon\right)\right] \geqq \underset{\rho\geqq 0}{\text{L.U.B.}} - \sqrt{\frac{2}{N}}\ln\frac{e}{\sqrt{P_{\min}}} + \rho\epsilon \tag{4.35}$$

Thus $E_{sp}$ is infinite here and (4.24) reduces to $P_{e,\max} \geqq 0$, completing the proof.

The theorem will now be generalized to lower bound the error prob-

ability for an arbitrary set of code words rather than a fixed composition set. The number of different ways to choose the composition of a code word is the number of ways of picking $K$ nonnegative integers, $N_1, N_2, \cdots, N_K$ such that $\sum_k N_k = N$, where $K$ is the input alphabet size and $N$ is the block length. Thus there are $\binom{N+K-1}{K-1}$ different compositions, and it follows that in any code of $M$ code words, there must be some composition containing a number of code words $M'$ bounded by

$$M' \geqq M \Big/ \binom{N+K-1}{K-1} \tag{4.36}$$

Consider the messages corresponding to this set of $M'$ words as a fixed composition code and assume that the same list decoding scheme is used as for the original code. Thus for each $m$ in the fixed composition set, $Y_m$ is the same as for the original code and $P_{e,m}$ is the same. This is presumably a rather foolish decoding scheme for the fixed composition code since the decoding lists might contain fewer than $L$ integers from the fixed composition set. None the less, Theorem 6 applies here, and using $\ln (M'/L)/N$ for $R$, there is some $m$ in the fixed composition set for which $P_{e,m}$ satisfies

$$P_{e,m} > \exp -N\left\{E_{sp}\left[\frac{\ln (M'/L)}{N} - \frac{\ln 4}{N} - \epsilon\right] + \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}\right\} \tag{4.37}$$

Since $E_{sp}$ is a decreasing function of its argument, we can substitute (4.36) into (4.37). Also $P_{e,m} \leqq P_{e,\max}$ for the original code, so that

$$P_{e,\max} > \exp -N\left\{E_{sp}\left[\frac{\ln (M/L) - \ln \binom{N+K-1}{K-1}}{N} - \frac{\ln 4}{N} - \epsilon\right] + \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}\right\} \tag{4.38}$$

For the given channel, define $P_{e,\max}(N, M, L)$ as the minimum $P_{e,\max}$ over all codes of $M$ code words of length $N$ and all list decoding schemes of list size $L$. Equation (4.38) clearly applies to the code and

decoding scheme that achieves $P_{e,\max}(N, M, L)$. Finally, since

$$\binom{N+K-1}{K-1} < N^K \tag{4.39}$$

We can rewrite (4.38) as

$$P_{e,\max}(N, M, L) > \exp -N\left\{E_{sp}\left[\frac{\ln (M/L)}{N} - \frac{K \ln N}{N} - \frac{\ln 4}{N}\right] + \sqrt{\frac{8}{N}} \ln \frac{e}{\sqrt{P_{\min}}} + \frac{\ln 4}{N}\right\} \tag{4.40}$$

We have chosen $\epsilon > 0$ to absorb the inequality in (4.39).

One more step will now complete the proof of Theorem 2. We show that, in general,

$$P_e(N, M, L) \geqq \tfrac{1}{2} P_{e,\max}(N, [M/2]^+, L) \tag{4.41}$$

To see this, consider the code that achieves the minimum average error probability $P_e(N, M, L)$. At least $M/2$ of these words must have $P_{e,m} \leqq 2P_e(N, M, L)$. This set of $[M/2]^+$ code words with the original decoding scheme then has $P_{e,\max} \leqq 2P_e(N, M, L)$. By definition, however, this $P_{e,\max}$ is greater than or equal to $P_{e,\max}(N, [M/2]^+, L)$, thus establishing (4.41).

Substituting (4.40) into (4.41), we obtain (1.6), thus completing the proof of Theorem 2.

In the proof of Theorem 2, it was not made quite clear why the artifice of fixed composition codes had to be introduced. We started the derivation of the bound by relating the error probability for a given message, $m$, to the size of the decoding subset $F(Y_m)$, and then observing that at least one $F(Y_m)$ must be at most $L/M$. This last observation, however, required that all $Y_m$ be measured with the same probability assignment $\mathbf{f}$. Unfortunately, a good choice of $\mathbf{f}$ for one code word composition is often a very poor choice for some other composition, and in general, no choice of $\mathbf{f}$ is uniformly good. We eventually chose $\mathbf{f}$ as a function of the parameter $s$, but the appropriate value of $s$ (i.e., that which satisfies (4.28) with equality) is a function of the code word composition $\mathbf{q}$, making $\mathbf{f}_s$ also implicitly dependent upon $\mathbf{q}$.

The reliance of the bound on fixed composition codes is particularly unfortunate in that it prevents us from extending the bound to continuous channels, channels with memory, and channels with feedback.

In the first case the size of the input alphabet $K$ becomes infinite, and in the other cases $\mu(s)$ in (4.4) depends on more than just the composition of a code word. One way to avoid these difficulties is to classify code words by the value of $s$ for which (4.28) is satisfied with equality but, so far, no *general* theorem has been proved using this approach. These extensions to more general channels are possible, however, if the channel has sufficient symmetry and we conjecture that the exponential bound $E_{sp}(R)$ is valid under much broader conditions than we have assumed here.

## APPENDIX

## PROPERTIES OF $E_{sp}(R)$

Using (1.7) and (1.8) we can rewrite $E_{sp}(R)$ as

$$E_{sp}(R) = \max_{\mathbf{q}} E(R, \mathbf{q}) \tag{A.1}$$

$$E(R, \mathbf{q}) = \underset{\rho \geqq 0}{\text{L.U.B.}} [E_0(\rho, \mathbf{q}) - \rho R] \tag{A.2}$$

Define $I(\mathbf{q})$ as the average mutual information on the channel using the input probabilities $(q_1, \cdots, q_K)$,

$$I(\mathbf{q}) = \sum_{k=1}^{K} \sum_{j=1}^{J} q_k P(j \mid k) \ln \frac{P(j \mid k)}{\sum_{i=1}^{K} q_i P(j \mid i)} \tag{A.3}$$

It has been shown by Gallager (1965, Theorem 2), that if $I(\mathbf{q}) \neq 0$, then

$$E_0(\rho, \mathbf{q}) \geqq 0 \tag{A.4}$$

$$0 < \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho} \leqq I(\mathbf{q}) \tag{A.5}$$

$$\frac{\partial^2 E_0(\rho, \mathbf{q})}{\partial \rho^2} \leqq 0 \tag{A.6}$$

with equality in (A.4) iff $\rho = 0$; in (A.5) if $\rho = 0$; and in (A.6) iff the following conditions are satisfied:

(a) $P(j \mid k)$ is independent of $k$ for those $j, k$ such that $q_k P(j \mid k) \neq 0$.

(b) The sum of the $q_k$ over inputs leading to output $j$ with nonzero probability is independent of $j$. It follows trivially from the same proof that $E_0(\rho, \mathbf{q}) = 0$ for all $\rho \geqq 0$ if $I(\mathbf{q}) = 0$.

Using these results, we can give $E(R, \mathbf{q})$ parametrically as

$$E(R, \mathbf{q}) = E_0(\rho, \mathbf{q}) - \rho \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho} \tag{A.7}$$

$$R = \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho} \tag{A.8}$$

Equations (A.7) and (A.8) are valid for

$$\lim_{\rho \to \infty} \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho} < R < \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho}\bigg|_{\rho=0} = I(\mathbf{q}) \tag{A.9}$$

also,

$$E(R, \mathbf{q}) = 0 \quad \text{if} \quad R \geqq I(\mathbf{q}) \tag{A.10}$$

$$E(R, \mathbf{q}) = \infty \quad \text{if} \quad R < \lim_{\rho \to \infty} \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho} \tag{A.11}$$

From (A.7) and (A.8), we have

$$\frac{\partial E(R, \mathbf{q})}{\partial R} = -\rho; \qquad R = \frac{\partial E_0(\rho, \mathbf{q})}{\partial \rho} \tag{A.12}$$

If (A.6) is satisfied with strict inequality, then $R$ in (A.8) is strictly decreasing with $\rho$ and from (A.12), $E(R, \mathbf{q})$ is strictly decreasing with $R$ and is strictly convex $\cup$ over the range of $R$ given by (A.9).

We now observe from (A.10) that if $R \geqq C = \max_{\mathbf{q}} I(\mathbf{q})$, then $E(R, \mathbf{q}) = 0$ for all $\mathbf{q}$ and $E_{sp}(R) = 0$. Also if $R < C$, then for the $\mathbf{q}$ that yields capacity, $E(R, \mathbf{q}) > 0$ and thus $E_{sp}(R) > 0$. Finally, for a given $R$ in the range $R_\infty < R < C$ the $\mathbf{q}$ that maximizes $E(R, \mathbf{q})$ satisfies (A.9), and thus $E_{sp}(R)$ is strictly decreasing and strictly convex $\cup$ in this range.

Next suppose that $R_{\text{crit}} = C$. Then for some $\rho^* \geqq 1$, $E_0(\rho^*)/\rho^* = C$, and thus for some $\mathbf{q}$, $E_0(\rho^*, \mathbf{q})/\rho^* = C$. But since $\partial E_0(\rho, \mathbf{q})/\partial \rho \leqq C$, this implies that $\partial E_0(\rho, \mathbf{q})/\partial \rho = C$ for $0 \leqq \rho \leqq \rho^*$ and $\partial^2 E_0(\rho, \mathbf{q})/\partial \rho^2 = 0$ for $0 \leqq \rho \leqq \rho^*$. From (A.6) this implies that conditions (a) and (b) above are satisfied for $\mathbf{q}$ yielding capacity. This in turn implies that $\partial E_0(\rho, \mathbf{q})/\partial \rho = C$ for all $\rho$ and thus $R_\infty = C$. The same argument shows that if $R_\infty = C$, conditions (a) and (b) above must be satisfied.

A Bound on $\mu_k''$

From (3.25), $\mu_k''(s)$ is the variance of the random variable $D_k(j) = \ln [f(j)/P(j/k)]$ with the probability assignment

$$Q_{sk}(j) = \frac{P(j/k)^{1-s} f(j)^s}{\sum_i P(i/k)^{1-s} f(i)^s} \tag{A.13}$$

If follows that $s^2\mu_k''(s)$ is the variance of $sD_k(j)$ with the same probability assignment. From (A.13), however, we see that

$$sD_k(j) = \ln \frac{Q_{sk}(j)}{P(j/k)} + \mu_k(s) \tag{A.14}$$

Thus $s^2\mu_k''(s)$ is also the variance of the random variable $\ln [Q_{sk}(j)/P(j/k)]$ with the probability assignment $Q_{sk}(j)$. Since a variance can be upper bounded by a second moment around any point, we have

$$s^2\mu_k''(s) \leqq \sum_j Q_{sk}(j) \left[ \ln \frac{Q_{sk}(j)}{P(j/k)} - \ln \frac{e}{\sqrt{P_{\min}}} \right]^2 \tag{A.15}$$

where $P_{\min}$ is the smallest nonzero transition probability on the channel and the sum is over those $j$ for which $P(j/k) > 0$.

We next upper bound the right hand side of (A.15) by maximizing over all choices of the probability vector $Q_{sk}(j)$. There must be a maximum since the function is continuous and the region is closed and bounded. The function cannot be maximized when any of the $Q_{sk}(j) = 0$, for the derivative with respect to such a $Q_{sk}(j)$ is infinite. Thus the maximum must be at a stationary point within the region, and any stationary point can be found by the LaGrange multiplier technique. This gives us, for each $j$,

$$\left[ \ln \frac{Q_{sk}(j)\sqrt{P_{\min}}}{P(j/k)e} \right]^2 + 2 \ln \frac{Q_{sk}(j)\sqrt{P_{\min}}}{P(j/k)e} + \lambda = 0 \tag{A.16}$$

Solving for the logarithmic term, we obtain

$$\ln \frac{Q_{sk}(j)\sqrt{P_{\min}}}{P(j/k)e} = -1 \pm \sqrt{1 - \lambda}; \quad \text{each} \quad j \tag{A.17}$$

There are two cases to consider: first where the same sign is used for the square root for each $j$; and second when the positive square root is used for some $j$ and the negative for others. In the first case, all terms on the left are equal, and $Q_{sk}(j) = P(j/k)$ to satisfy the constraint that $Q_{sk}(j)$ is a probability vector. Then (A.15) reduces to

$$s^2\mu_k''(s) \leqq \left[\ln \frac{e}{\sqrt{P_{\min}}}\right]^2 \tag{A.18}$$

In the second case, the left hand side of (A.17) is upper bounded by $Q_{sk}(j) = 1$, $P(j/k) = P_{\min}$, yielding $-\ln e\sqrt{P_{\min}}$. From the right hand side of (A.17), the terms using the negative square root can have a magnitude at most 2 larger than the positive term. Thus

$$\left|\ln \frac{Q_{sk}(j)\sqrt{P_{\min}}}{P(j/k)e}\right| \leqq 2 - \ln e\sqrt{P_{\min}} = \ln \frac{e}{\sqrt{P_{\min}}} \tag{A.19}$$

Substituting (A.19) into (A.15) again yields (A.18) completing the proof.

PROOF THAT $\mathbf{q}_s$, $\mathbf{f}_s$ YIELDS A SADDLE POINT FOR $q_k\mu_k(s, \mathbf{f})$ (SEE (4.23))

From (4.22), we see that the right side of (4.23) is valid and also that

$$\sum_k q_{ks}\mu_k(s, \mathbf{f}_s) = (1 - s) \ln \sum_j \alpha_{js}^{1/(1-s)}. \tag{A.20}$$

In order to establish the left side of (4.23) we must show that

$$\sum_k q_{ks} \ln \left[\sum_j P(j \mid k)^{1-s} f(j)^s\right] - (1 - s) \ln \sum_j \alpha_{js}^{1/(1-s)} \leqq 0 \tag{A.21}$$

Combining the logarithm terms, and using the inequality $\ln z \leqq z - 1$ for $z \geqq 0$ (taking $\ln 0$ as $-\infty$), the left side of (A.21) becomes

$$\sum_k q_{ks} \ln \frac{\sum_j P(j \mid k)^{1-s} f(j)^s}{(\sum_j \alpha_{js}^{1/(1-s)})^{1-s}} \leqq \frac{\sum_{k,j} q_{ks} P(j \mid k)^{1-s} f(j)^s}{(\sum_j \alpha_{js}^{1/(1-s)})^{1-s}} - 1 \tag{A.22}$$

$$\leqq \sum_j f_s(j)^{1-s} f(j)^s - 1 \tag{A.23}$$

$$\leqq 0 \tag{A.24}$$

when we have used (4.19) and then (4.20) to go from (A.22) to (A.23), and used Holder's inequality to go from (A.23) to (A.24). This completes the proof.

PROOF THAT $R(s, \mathbf{q})$ (SEE (4.25)) IS CONTINUOUS IN $s$, $0 < s < 1$

The problem here is to show that $\mathbf{f}_s$ is a continuous vector function of $s$. It will then follow immediately that $\mu_k(s, \mathbf{f}_s)$ and $\mu_k'(s, \mathbf{f}_s)$ are continuous functions of $s$, and then from (4.25) that $R(s, \mathbf{q})$ is a continuous function of $s$ for fixed $\mathbf{q}$.

$E_0(\rho, \mathbf{q})$ as given by (1.9) can be rewritten as

$$E_0\left(\frac{s}{1-s}, \mathbf{q}\right) = -\ln \sum_j \alpha_j(s, \mathbf{q})^{1/(1-s)} \tag{A.25}$$

$$\alpha_j(s, \mathbf{q}) = \sum_k q_k P(j \mid k)^{1-s} \tag{A.26}$$

Let $\mathbf{q}_s$ be a choice of probability vector $\mathbf{q}$ that maximizes $E_0(s/(1-s), \mathbf{q})$. We show that $\alpha_j(s, \mathbf{q}_s)$, which is $\alpha_{js}$ as defined in (4.19), is a continuous function of $s$, and it then follows from (4.20) that $\mathbf{f}_s$ is a continuous function of $s$. Since $\mathbf{q}_s$ maximizes $E_0(s/(1-s), \mathbf{q})$, we have

$$E_0\left(\frac{s}{1-s}, \mathbf{q}_s\right) = -\ln \min_{\boldsymbol{\alpha}(s,\mathbf{q})} \sum_j \alpha_j(s, \mathbf{q})^{1/(1-s)} \tag{A.27}$$

where the minimization is over the set of vectors $\boldsymbol{\alpha}$ whose components satisfy (A.26) for some choice of probability vector $\mathbf{q}$. Since this is a convex set of vectors and since $\sum_j \alpha_j^{1/(1-s)}$ is a *strictly* convex $\cup$ function of $\boldsymbol{\alpha}$ for $0 < s < 1$, the minimizing $\boldsymbol{\alpha}$ in (A.27) is unique and the strict convexity tells us that for any $s$, $0 < s < 1$ and for any $\epsilon > 0$ there exists a $\delta > 0$ such that if

$$| \alpha_j(s, \mathbf{q}) - \alpha_j(s, \mathbf{q}_s) | \geq \epsilon/2; \qquad \text{any } j \tag{A.28}$$

then

$$\sum_j \alpha_j(s, \mathbf{q})^{1/(1-s)} \geq \sum_j \alpha_j(s, \mathbf{q}_s)^{1/(1-s)} + \delta \tag{A.29}$$

Next we observe that $E_0(s/(1-s), \mathbf{q})$ is a continuous function of $s$ with the continuity being uniform in $\mathbf{q}$. It follows from this that $E_0(s/(1-s), \mathbf{q}_s)$ is also continuous in $s$. Also $\alpha_j(s, \mathbf{q})$ is continuous in $s$, uniformly in $\mathbf{q}$. It follows from these three statements that for a given $s$, $0 < s < 1$, and for the given $\epsilon$, $\delta$ above, there exists a $\delta_1 > 0$ such that for $| s_1 - s | < \delta_1$,

$$| \sum_j \alpha_j(s_1, \mathbf{q}_{s_1})^{1/(1-s_1)} - \sum_j \alpha_j(s, \mathbf{q}_{s_1})^{1/(1-s)} | < \delta/2 \tag{A.30}$$

$$| \sum_j \alpha_j(s_1, \mathbf{q}_{s_1})^{1/(1-s_1)} - \sum_j \alpha_j(s, \mathbf{q}_s)^{1/(1-s)} | < \delta/2 \tag{A.31}$$

$$| \alpha_j(s_1, \mathbf{q}_{s_1}) - \alpha_j(s, \mathbf{q}_{s_1}) | < \epsilon/2; \qquad \text{all } j \tag{A.32}$$

Combining (A.30) and (A.31), we see that (A.29) is unsatisfied for $\mathbf{q} = \mathbf{q}_{s_1}$; thus (A.28) must be unsatisfied for all $j$ and

$$| \alpha_j(s, \mathbf{q}_{s_1}) - \alpha_j(s, \mathbf{q}_s) | < \epsilon/2; \qquad \text{all } j, \ | s - s_1 | < \delta_1 \tag{A.33}$$

Combining (A.32) and (A.33), we then have for all $j$

$$| \alpha_j(s_1, \mathbf{q}_{s_1}) - \alpha_j(s, \mathbf{q}_s) | < \epsilon; \qquad | s - s_1 | < \delta_1 \tag{A.34}$$

Thus $\alpha_j(s, \mathbf{q}_s)$ is continuous in $s$, completing the proof. Using other methods, it can be shown that $\alpha_j(s, \mathbf{q}_s)$ is a piecewise analytic function of $s$.

RECEIVED: January 18, 1966

## REFERENCES


ASH, R. B. (1965), "Information Theory." Interscience, New York.

BERLEKAMP, E. R. (1964), "Block Coding with Noiseless Feedback." Ph.D. Thesis, Department of Electrical Engineering, M.I.T.

BHATTACHARYYA, A. (1943), On a measure of divergence between two statistical populations defined by their probability distributions. *Bull. Calcutta Math. Soc.* **35,** No. 3, 99–110.

CHERNOFF, H. (1952), A measure of asymptotic efficiency for tests of an hypothesis based on the sum of observations. *Ann. Math. Statist.* **23,** 493.

ELIAS, P. (1955), "List Decoding for Noisy Channels." Tech. Rept. 335, Research Laboratory of Electronics, M.I.T.

FANO, R. M. (1961), "Transmission of Information." M.I.T. Press, and Wiley, New York.

FEINSTEIN, A. (1955), Error bounds in noisy channels without memory. *IEEE Trans. Inform. Theory* **IT-1,** 13–14.

FELLER, W. (1943), Generalizations of a probability limit theorem of Cramer. *Trans. Am. Math. Soc.* **54,** 361.

GALLAGER, R. (1963), "Low Density Parity Check Codes." M.I.T. Press.

GALLAGER, R. (1965a), A simple derivation of the coding theorem and some applications. *IEEE Trans. Inform. Theory* **IT-11,** 3–18.

GALLAGER, R. (1965), "Lower Bounds on the Tails of Probability Distributions." M.I.T. Research Laboratory of Electronics. OPR **77,** pp. 277–291.

GILBERT, E. N. (1952), A comparison of signalling alphabets. *Bell System Tech. J.* **3,** 504–522.

HAMMING, R. W. (1950), Error detecting and error correcting codes. *Bell System Tech. J.* **29,** 47–160.

HELLIGER, E. (1909), Neue Begrundung der Theorie quadratischer Formen von unendlichvielen Veranderlichen. *J. reine angew. Math.* **136,** 210–271.

JACOBS, I. M., AND BERLEKAMP, E. R. (1967), A lower bound to the distribution of computation for sequential decoding. *IEEE Trans. Inform. Theory* **IT-13,** in press.

NEYMAN, J. AND PEARSON, E. S. (1928), On the use and interpretation of certain test criterion for purposes of statistical inference, *Biometrica* **20A,** 175, 263.

PETERSON, W. W. (1961), "Error-Correcting Codes." M.I.T. Press, and Wiley, New York.

PLOTKIN, M. (1960), Research Division Report 51–20, University of Pennsylvania.

Published in 1960 as: Binary codes with specified minimum distance. *IEEE Trans. Inform. Theory* **IT-6**, 445–450.

REIFFEN, B. (1963), A note on "very noisy" channels. *Inform. and Control* **6**, 126–130.

SHANNON, C. E. (1948), A mathematical theory of communication. *Bell System Tech. J.* **27**, 379, 623. Also in book form with postscript by W. Weaver, Univ. of Illinois Press, Urbana, Illinois.

SHANNON, C. E. (1956), Zero error capacity of noisy channels. *IEEE Trans. Inform. Theory* **IT-2**, 8.

SHANNON, C. E. (1958), Certain results in coding theory for noisy channels. *Inform. Control* **1**, 6.

SUN, M. (1965), Asymptotic bounds on the probability of error for the optimal transmission of information in the channel without memory which is symmetric in pairs of input symbols for small rates of transmission. *Theory Probab. Appl.* (Russian) **10**, no. 1, 167–175.