A Simple Derivation of the Coding Theorem and Some Applications

ROBERT G. GALLAGER, MEMBER, IEEE

Abstract—**Upper bounds are derived on the probability of error that can be achieved by using block codes on general time-discrete memoryless channels. Both amplitude-discrete and amplitude-continuous channels are treated, both with and without input constraints. The major advantages of the present approach are the simplicity of the derivations and the relative simplicity of the results; on the other hand, the exponential behavior of the bounds with block length is the best known for all transmission rates between 0 and capacity. The results are applied to a number of special channels, including the binary symmetric channel and the additive Gaussian noise channel.**

I. Introduction

THE CODING THEOREM, discovered by Shannon [1] in 1948, states that for a broad class of communication channel models there is a maximum rate, capacity, at which information can be transmitted over the channel, and that for rates below capacity, information can be transmitted with arbitrarily low probability of error.

For discrete memoryless channels, the strongest known form of the theorem was stated by Fano [2] in 1961. In this result, the minimum probability of error P_e for codes of block length N is bounded for any rate below capacity[1] between the limits

$$e^{-N[E_L(R)+0(N)]} \leq P_e \leq 2e^{-NE(R)} \tag{1}$$

In this expression, $E_L(R)$ and $E(R)$ are positive functions of the channel transition probabilities and of the rate R; $0(N)$ is a function going to 0 with increasing N. For a range of rates immediately beneath channel capacity, $E_L(R) = E(R)$.

The function $E(R)$, especially in the range in which $E(R) = E_L(R)$, appears to yield a fundamental characterization of a channel for coding purposes. It brings out clearly and simply the relationships between error probability, data rate, constraint length, and channel behavior. Recent advances in coding theory have yielded a number of effective and economically feasible coding techniques, and (1) provides a theoretical framework within which to discuss intelligently the relative merits of these techniques. Even more important, the function $E(R)$ provides a more meaningful comparison between different channels than can be made on the basis of capacity or SNR. For example, if one is to use coding on a physical communication link, one of the first questions to be answered involves the type of digital modulation systems to use. Considering the modulation system as part of the channel, one can compare modulation systems for coding applications on the basis of their $E(R)$ curves. For an example of such a comparison, see Wozencraft and Kennedy [4].

In Section II of this paper, a simple proof is given that $P_e < e^{-NE(R)}$. In Section III, we establish a number of properties of $E(R)$ and show explicitly how the function $E(R)$ can be calculated. This calculation is just slightly more complicated than the calculation of channel capacity. In Section IV, we give a number of applications of the theory developed in Sections II and III. First, as an example, we derive $E(R)$ for a binary symmetric channel; then we derive a universal $E(R)$ curve for very noisy channels; and finally, we relate $E(R)$ for a set of parallel channels to the $E(R)$ curves of the individual channels.

In Section V, we derive an improved upper bound to P_e for low rates; this yields a larger value of $E(R)$ than was derived in Section II. There is some reason to suspect that the combination of these two bounds produces the true exponential behavior with block length of the best codes. In Section VI, these results are extended to channels with constraints on the input and to channels with continuous input and output alphabets. Finally, the results are applied to the additive Gaussian noise channel as an example.

II. Derivation of the Coding Theorem

Let X_N be the set of all sequences of length N that can be transmitted on a given channel, and let Y_N be the set of all sequences of length N that can be received. We assume that both X_N and Y_N are finite sets. Let $Pr\ (\mathbf{y} \mid \mathbf{x})$, for $\mathbf{y} \in Y_N$ and $\mathbf{x} \in X_N$, be the conditional probability of receiving sequence $\mathbf{y}$, given that $\mathbf{x}$ was transmitted. We assume that we have a code consisting of M code words; that is, a mapping of the integers from 1 to M into a set of code words $\mathbf{x}_1, \cdots, \mathbf{x}_M$, where $\mathbf{x}_m \in X_N$; $1 \leq m \leq M$. We assume that maximum likelihood decoding is performed at the receiver; that is, the decoder decodes the output sequence $\mathbf{y}$ into the integer m if

$$Pr(\mathbf{y}|\mathbf{x}_m) > Pr(\mathbf{y}_m|\mathbf{x}) \text{ for all } m' \neq m,\ 1 \leq m' \leq M \tag{2}$$

Manuscript received March 11, 1964. This work was supported in part by the U. S. Army, Navy, and Air Force under Contract DA36-039-AMC-03200(E); and in part by the National Science Foundation (Grant GP-2495), the National Institutes of Health (Grant MH-04737-04), and the National Aeronautics and Space Administration (Grants NsG-334 and NsG-496).

The author is with the Dept. of Electrical Engineering and the Research Lab. of Electronics, Massachusetts Institute of Technology, Cambridge, Mass.

[1] This paper deals only with error probabilities at rates below capacity. For the strongest known results at rates above capacity, see Gallager [3], Section 6.

For purposes of overbounding the probability of decoding error, we regard any situation in which no m satisfies (2) as a decoding error. Also, of course, a decoding error is made if the decoded integer is different from the input integer. Now let P_{em} be the probability of decoding error when $\mathbf{x}_m$ is transmitted. A decoding error will be made if a $\mathbf{y}$ is received such that (2) is not satisfied. Thus we can express P_{em} as

$$P_{em} = \sum_{\mathbf{y}\in Y_N} Pr(\mathbf{y}|\mathbf{x}_m)\phi_m(\mathbf{y}) \tag{3}$$

where we define the function $\phi_m(\mathbf{y})$ as

$$\phi_m(\mathbf{y}) = 1 \text{ if } Pr(\mathbf{y}|\mathbf{x}_m) \le Pr(\mathbf{y}|\mathbf{x}_{m'}) \text{ for some } m' \neq m \tag{4}$$

$$\phi_m(\mathbf{y}) = 0 \text{ otherwise} \tag{5}$$

We shall now upperbound P_{em} by upperbounding the function $\phi_m(\mathbf{y})$:

$$\phi_m(\mathbf{y}) \le \left[\frac{\sum_{m'\neq m} Pr(\mathbf{y}|\mathbf{x}_{m'})^{1/(1+\rho)}}{Pr(\mathbf{y}|\mathbf{x}_m)^{1/(1+\rho)}}\right]^{\rho} \quad \rho > 0 \tag{6}$$

The reason for using (6) is not at all obvious intuitively, but we can at least establish its validity by noting that the right-hand side of (6) is always non-negative, thereby satisfying the inequality when $\phi_m(\mathbf{y}) = 0$. When $\phi_m(\mathbf{y}) = 1$, some term in the numerator is greater than or equal to the denominator, thus the numerator is greater than or equal to the denominator; raising the fraction to the ρ power keeps it greater than or equal to 1. Substituting (6) in (3), we have

$$P_{em} \le \sum_{\mathbf{y}\in Y_N} Pr(\mathbf{y}|\mathbf{x}_m)^{1/(1+\rho)}\left[\sum_{m'\neq m} Pr(\mathbf{y}|\mathbf{x}_{m'})^{1/(1+\rho)}\right]^{\rho}$$
$$\text{for any } \rho > 0 \tag{7}$$

Equation (7) yields a bound to P_{em} for a particular set of code words. Aside from certain special cases, this bound is too complicated to be useful if the number of code words is large. We will simplify (7) by averaging over an appropriately chosen ensemble of codes. Let us suppose that we define a probability measure $P(\mathbf{x})$ on the set X_N of possible input sequences to the channel. We can now generate an ensemble of codes by picking each code word, independently, according to the probability measure $P(\mathbf{x})$. Thus the probability associated with a code consisting of the code words $\mathbf{x}_1, \cdots, \mathbf{x}_M$ is $\prod_{m=1}^{M} P(\mathbf{x}_m)$. Clearly, at least one code in the ensemble will have a probability of error that is as small as the ensemble-average probability of error. Using a bar to represent code ensemble averages, we now have

$$\bar{P}_{em} \le \overline{\overset{1}{\sum_{\mathbf{y}\in Y_N}} Pr(\mathbf{y}|\mathbf{x}_m)^{1/(1+\rho)} \overset{2}{\,} \left[\overset{4}{\sum_{m'\neq m}} Pr(\mathbf{y}|\mathbf{x}_{m'})^{1+\rho}\right]^{\rho}\overset{3}{\,}} \tag{8}$$

We now impose the additional restriction that $\rho \le 1$, and proceed to remove the numbered portions of the averaging bar in (8). First, observe that all of the terms of (8) under the bar are random variables; that is, they are real valued functions of the set of randomly chosen words. Thus we can remove part 1 of the bar in (8), since the average of a sum of random variables is equal to the sum of the averages. Likewise, we can remove part 2, because the average of the product of *independent* random variables is equal to the product of the averages. The independence comes from the fact that the code words are chosen independently.

To remove part 3, let ξ be the random variable in brackets; we wish to show that $\overline{\xi^{\rho}} \le \bar{\xi}^{\rho}$. Figure 1 shows ξ^{ρ}, and it is clear that for $0 < \rho \le 1$, ξ^{ρ} is a convex upward function of ξ; i.e., a function whose chords all lie on or beneath the function.[2] Figure 1 illustrates that $\overline{\xi^{\rho}} \le \bar{\xi}^{\rho}$ for the special case in which ξ takes on only two values, and the general case is a well-known result.[3] Part 4 of the averaging bar can be removed by the interchange of sum and average. Thus[4]

$$\bar{P}_{em} \le \sum_{\mathbf{y}\in Y_N} \overline{Pr(\mathbf{y}|\mathbf{x}_m)^{1/(1+\rho)}}\left[\sum_{m'\neq m} \overline{Pr(\mathbf{y}|\mathbf{x}_{m'})^{1/(1+\rho)}}\right]^{\rho} \tag{9}$$

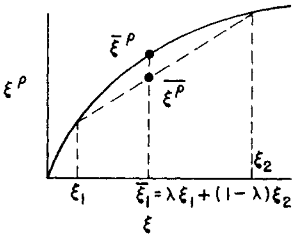


Fig. 1. Convexity of ξ^{ρ}.

Since the code words are chosen with the probability $P(\mathbf{x})$,

$$\overline{Pr(\mathbf{y}|\mathbf{x}_m)^{1/(1+\rho)}} = \sum_{\mathbf{x}\in X_N} P(\mathbf{x})Pr(\mathbf{y}|\mathbf{x})^{1/(1+\rho)} \tag{10}$$

Observing that the right-hand side of (10) is independent of m, we can substitute (10) in both the m and m' term in (9). Since the summation in (9) is over $M - 1$ terms, this yields

$$\bar{P}_{em} \le (M-1)^{\rho} \sum_{\mathbf{y}\in Y_N}\left[\sum_{\mathbf{x}\in X_N} P(\mathbf{x})Pr(\mathbf{y}|\mathbf{x})^{1/(1+\rho)}\right]^{1+\rho}$$
$$\text{for any } \rho,\ 0 < \rho \le 1 \tag{11}$$

The bound in (11) applies to any discrete channel,

[2] Let $f(\mathbf{x})$ be a real valued function of a vector $\mathbf{x}$ over a region R. We call the region convex if for any $\mathbf{x}_1 \epsilon R$, $\mathbf{x}_2 \epsilon R$; and λ, $0 < \lambda < 1$, we have $\lambda\mathbf{x}_1 + (1-\lambda)\mathbf{x}_2 \epsilon R$. The function $f(\mathbf{x})$ is convex upward over the convex region if for any $\mathbf{x}_1 \epsilon R$, $\mathbf{x}_2 \epsilon R$, and $0 < \lambda < 1$ we have $\lambda f(\mathbf{x}_1) + (1-\lambda)f(\mathbf{x}_2) \le f[\lambda\mathbf{x}_1 + (1-\lambda)\mathbf{x}_2]$. The function is strictly convex if the inequality, $\le$, can be replaced with strict inequality, $<$.

[3] See, for example, Blackwell and Girshick [5], page 38.

[4] By a minor modification of the argument used here, only pair-wise independence in the code-word selection is necessary to get from (8) to (9). This makes it possible to apply the bounds developed here to special ensembles of codes such as parity check code ensembles.

memoryless or not, for which $Pr\ (\mathbf{y} \mid \mathbf{x})$ can be defined. It is valid for all choices of $P(\mathbf{x})$ and all ρ, $0 < \rho \le 1$.

We shall now assume that the channel is memoryless so as to simplify the bound in (11). Let $x_1, \cdots, x_n, \cdots, x_N$ be the individual letters in an input sequence $\mathbf{x}$, and let $y_1, \cdots, y_n, \cdots, y_N$ be the letters in a sequence $\mathbf{y}$. By a memoryless channel, we mean a channel that satisfies

$$Pr(\mathbf{y}|\mathbf{x}) = \prod_{n=1}^{N} Pr(y_n|x_n) \tag{12}$$

for all $\mathbf{x}\ \varepsilon\ X_N$ and $\mathbf{y}\ \varepsilon\ Y_N$ and all N. Now we restrict the class of ensembles of codes under consideration to those in which each letter of each code word is chosen independently of all other letters with a probability measure $p(x)$; $x\ \varepsilon\ X_1$.

$$P(x) = \prod_{n=1}^{N} p(x_n); \qquad x = (x_1, \cdots, x_n, \cdots, x_N) \tag{13}$$

Substituting (12) and (13) in (11), we get

$$\bar{P}_{em} \le (M-1)^{\rho} \sum_{\mathbf{y}\varepsilon Y_N} \left[\sum_{\mathbf{x}\varepsilon X_N} \prod_{n=1}^{N} p(x_n)\, Pr\ (y_n \mid x_n)^{1/(1+\rho)} \right]^{1+\rho} \tag{14}$$

We can rewrite the bracketed term in (14) to get

$$\bar{P}_{em} \le (M-1)^{\rho} \sum_{\mathbf{y}\varepsilon Y_N} \left[\prod_{n=1}^{N} \sum_{x_n \varepsilon X_1} p(x_n)\, Pr\ (y_n \mid x_n)^{1/(1+\rho)} \right]^{1+\rho} \tag{15}$$

Note that the bracketed term in (15) is a product of sums and is equal to the bracketed term in (14) by the usual arithmetic rule for multiplying products of sums. Finally, taking the product outside the brackets in (15), we can apply the same rule again to get

$$\bar{P}_{em} \le (M-1)^{\rho} \prod_{n=1}^{N} \sum_{y_n \varepsilon Y_1} \left[\sum_{x_n \varepsilon X_1} p(x_n)\, Pr\ (y_n \mid x_n)^{1/(1+\rho)} \right]^{1+\rho} \qquad 0 < \rho \le 1 \tag{16}$$

We can simplify the notation in (16) somewhat by observing that X_1 is the set of input letters, which is denoted $a_1, \cdots a_k, \cdots a_K$, where K is the size of the channel input alphabet. Also, Y_1 is the set of output letters, denoted $b_1, \cdots, b_j, \cdots b_J$, where J is the size of the output alphabet. Now let P_{jk} denote the channel transition probability $Pr\ (b_j \mid a_k)$ and let $p(a_k) = p_k$ denote the probability with which letter a_k is chosen in the code ensemble. Substituting this notation in (16), noting that all terms in the product are identical, and including the trivial case $\rho = 0$, we get

$$\bar{P}_{em} \le (M-1)^{\rho} \left[\sum_{j=1}^{J} \left(\sum_{k=1}^{K} p_k\, P_{jk}^{\ 1/(1+\rho)} \right)^{1+\rho} \right]^{N} \qquad 0 \le \rho \le 1 \tag{17}$$

If we now upperbound $M - 1$ by $M = e^{NR}$, where R is the code rate in nats per channel symbol, (17) can be rewritten as

$$\bar{P}_{em} \le \exp - N \left[-\rho R - ln \sum_{j=1}^{J} \left(\sum_{k=1}^{K} p_k\, P_{jk}^{\ 1/(1+\rho)} \right)^{1+\rho} \right] \tag{18}$$

Since the right-hand side of (18) is independent of m, it is a bound on the ensemble probability of decoding error and is independent of the probabilities with which the code words are used. Since at least one code in the ensemble must have an error probability as small as the average,[5] we have proved the following fundamental theorem:

Theorem 1

Consider a discrete memoryless channel with an input alphabet of K symbols, $a_1, \cdots a_K$; an output alphabet of J symbols, $b_1, \cdots b_J$; and transition probabilities $P_{jk} = Pr\ (b_j \mid a_k)$. For any block length N, any number of code words $M = e^{NR}$, and any probability distribution on the use of the code words, there exists a code for which the probability of decoding error is bounded by

$$P_e \le \exp - N[-\rho R + E_0(\rho, \mathbf{p})] \tag{19}$$

$$E_0(\rho, \mathbf{p}) = - ln \sum_{j=1}^{J} \left(\sum_{k=1}^{K} p_k\, P_{jk}^{\ 1/(1+\rho)} \right)^{1+\rho} \tag{20}$$

where ρ is an arbitrary number, $0 \le \rho \le 1$, and $\mathbf{p} = (p_1, p_2, \cdots, p_K)$ is an arbitrary probability vector.[6]

Theorem 1 is valid for all ρ, $0 \le \rho \le 1$, and all probability vectors $\mathbf{p} = (p_1, \cdots, p_K)$; thus we get the tightest bound on P_e by minimizing over ρ and $\mathbf{p}$. This gives us the trivial corollary:

Corollary 1: Under the same conditions as Theorem 1, there exists a code for which

$$P_e \le \exp - NE(R) \tag{21}$$

$$E(R) = \max_{\rho, \mathbf{p}}\ [-\rho R + E_0(\rho, \mathbf{p})] \tag{22}$$

where the maximization is over all ρ, $0 \le \rho \le 1$, and all probability vectors, $\mathbf{p}$.

The function $E(R)$ is the reliability curve discussed in the last section. Except for small values of R (see Section V), Corollary 1 provides the tightest known general bound on error probability for the discrete memoryless channel. We discuss the properties of $E(R)$ in Section III and, in particular, show that $E(R) > 0$ for $0 \le R < C$, where C is the channel capacity.

It is sometimes convenient to have a bound on error probability that applies to each code word separately rather than to the average.

Corollary 2: Under the same conditions as Theorem 1, there exists a code such that, for all m, $1 \le m \le M$, the probability of error when the mth code word is transmitted is bounded by

[5] The same code might not satisfy (18) for all choices of probabilities with which to use the code words; see Corollary 2.

[6] A probability vector is a vector whose components are all non-negative and sum to one.

$$P_{em} \leq 4e^{-NE(R)} \tag{23}$$

where $E(R)$ is given by (22).

Proof: Pick a code with $M' = 2M$ code words which satisfies Corollary 1 when the source uses the $2M$ code words with equal probability. [The rate, R' in (21) and (22) is now $(\ln 2M)/N$.] Remove the M words in the code for which P_{em} is largest. It is impossible for over half the words in the code to have an error probability greater than twice the average; therefore the remaining code words must satisfy

$$P_{em} \leq 2e^{-NE(R')} \tag{24}$$

Since $R' = (\ln 2M)/N = R + (\ln 2)/N$, and since $0 \leq \rho \leq 1$, (22) gives us

$$E(R') \geq E(R) - \frac{\ln 2}{N} \tag{25}$$

Substituting (25) in (24) gives us (23), thereby completing the proof.

III. Properties of the Reliability Curve, $E(R)$

The maximization of (22) over ρ and $\mathbf{p}$ depends on the behavior of the function $E_0(\rho, \mathbf{p})$. Theorem 2 describes $E_0(\rho, \mathbf{p})$ as a function of ρ, and Theorem 3 describes $E_0(\rho, \mathbf{p})$ as a function of $\mathbf{p}$. Both theorems are proved in the Appendix.

Theorem 2

Consider a channel with K inputs, J outputs, and transition probabilities

$$P_{jk}, \ 1 \leq k \leq K$$

Let $\mathbf{p} = (p_1, \cdots, p_K)$ be a probability vector on the channel inputs, and assume that the average mutual information

$$I(\mathbf{p}) = \sum_{k=1}^{K} \sum_{j=1}^{J} p_k P_{jk} \ln \frac{P_{jk}}{\sum_{i=1}^{K} p_i P_{ji}}$$

is nonzero. Then, for $\rho \geq 0$,

$$E_0(\rho, \mathbf{p}) = 0 \qquad \text{for} \quad \rho = 0 \tag{26}$$

$$E_0(\rho, \mathbf{p}) > 0 \qquad \text{for} \quad \rho > 0 \tag{27}$$

$$\frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} > 0 \qquad \text{for} \quad \rho > 0 \tag{28}$$

$$\left. \frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} \right|_{\rho=0} = I(\mathbf{p}) \tag{29}$$

$$\frac{\partial^2 E_0(\rho, \mathbf{p})}{\partial \rho^2} \leq 0 \tag{30}$$

with equality in (30) if and only if both of the following conditions are satisfied:

1) P_{jk} is independent of k for j, k such that $p_k P_{jk} \neq 0$
2) $\sum_{k; P_{jk} \neq 0} p_k$ is independent of j.

Using this theorem, we can easily perform the maximization of (22) over ρ for a given $\mathbf{p}$. Define

$$E(R, \mathbf{p}) = \max_{0 \leq \rho \leq 1} [-\rho R + E_0(\rho, \mathbf{p})] \tag{31}$$

Setting the partial derivative of the bracketed part of (31) equal to 0, we get

$$R = \frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} \tag{32}$$

From (30), if some ρ in the range $0 \leq \rho \leq 1$ satisfies (32), then that ρ must maximize (31). Furthermore, from (30) $\partial E_0(\rho, \mathbf{p})/\partial \rho$ is nonincreasing with ρ, so that a solution to (32) exists if R lies in the range

$$\left. \frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} \right|_{\rho=1} \leq R \leq I(\mathbf{p}) \tag{33}$$

In this range it is most convenient to use (32) to relate $E(R, \mathbf{p})$ and R parametrically as functions of ρ. This gives us

$$E(R, \mathbf{p}) = E_0(\rho, \mathbf{p}) - \rho \frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} \tag{34}$$

$$R = \frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} \qquad 0 \leq \rho \leq 1 \tag{35}$$

Figure 2 gives a graphical construction for the solution of these parametric equations.

For $R < \partial E_0(\rho, \mathbf{p})/\partial \rho \,|_{\rho=1}$, the parametric equations (34) and (35) are not valid. In this case, the function $-\rho R + E_0(\rho, \mathbf{p})$ increases with ρ in the range $0 \leq \rho \leq 1$, and therefore the maximum occurs at $\rho = 1$. Thus

$$E(R, \mathbf{p}) = E_0(1, \mathbf{p}) - R \quad \text{for} \quad R < \left. \frac{\partial E_0(\rho, \mathbf{p})}{\partial \rho} \right|_{\rho=1} \tag{36}$$

The behavior of $E(R, \mathbf{p})$ as a function of R given by (34)–(36) is shown in Fig. 3; this behavior depends upon whether $\partial^2 E_0(\rho, \mathbf{p})/\partial \rho^2$ is negative or 0. If it is negative, then R as given by (35) is strictly decreasing with ρ. Differentiating (34) with respect to ρ, we get $-\rho \, \partial^2 E_0(\rho, \mathbf{p})/\partial \rho^2$; thus $E(R, \mathbf{p})$ is strictly increasing with ρ for $\rho \geq 0$, and is equal to 0 for $\rho = 0$. Thus if $R < I(\mathbf{p})$, then $E(R, \mathbf{p}) > 0$. If $\mathbf{p}$ is chosen to achieve capacity, C, then for $R < C$, $E(R, \mathbf{p}) > 0$, and the error probability can be made to vanish exponentially with the block length.

Taking the ratio of the derivatives of (34) and (35), we see that

$$\frac{\partial E(R, \mathbf{p})}{\partial R} = -\rho \tag{37}$$

Thus the parameter ρ in (34) and (35) has significance as the negative slope of the E, R curve.

From the conditions following (30), it is clear that if $\partial^2 E_0(\rho, \mathbf{p})/\partial \rho^2 = 0$ for one value of $\rho > 0$, it is 0 for all $\rho > 0$. Under these circumstances, R and $E(R, \mathbf{p})$ as given by (34) and (35) simply specify the point at which $R = I(\mathbf{p})$, $E(R, \mathbf{p}) = 0$. The rest of the curve, as shown in Fig. 4, comes from (36).

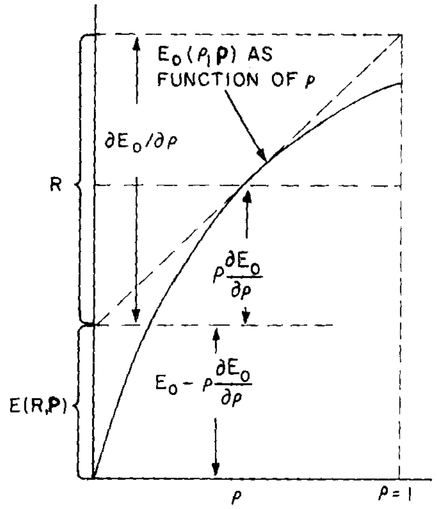


Fig. 2. Geometric construction of $E(R, \mathbf{p})$.

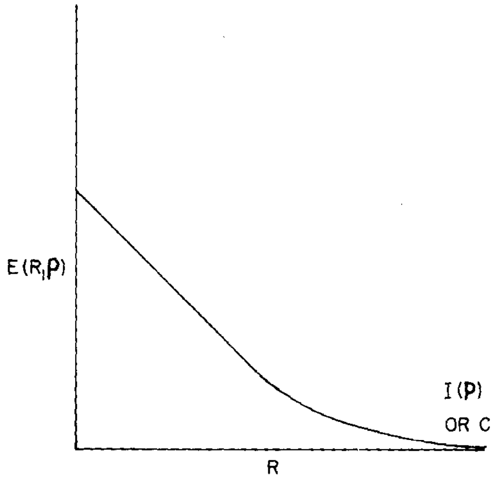


Fig. 3. Exponent, rate curve.

The class of channels for which $\partial^2 E_0(\rho, \mathbf{p})/\partial\rho^2 = 0$ is somewhat pathological. It includes noiseless channels, for which one can clearly achieve zero error probability at rates below capacity. The exponential bounds here simply reflect the probability of assigning more than one message to the same code word. The bound in Section V yields zero error probability in these cases. As an example of a noisy channel with $\partial^2 E_0(\rho, \mathbf{p})/\partial\rho^2 = 0$, see Fig. 4.

An alternative approach to the maximization of (31) over ρ is to regard the function $-\rho R + E_0(\rho, \mathbf{p})$ as a linear function of R with slope $-\rho$ and intercept $E_0(\rho, \mathbf{p})$ for fixed ρ. Thus $E(R, \mathbf{p})$ as a function of R is simply the upper envelope of this set of straight lines (see Fig. 5). (In this paper, the upper envelope of a set of lines will be taken to mean the lowest upper bound to that set of lines.) This picture also interprets $E_0(\rho, \mathbf{p})$ as the E-axis intercept of the tangent of slope $-\rho$ to the E, R curve.

Since $E(R, \mathbf{p})$ is the upper envelope of a set of straight lines, it must be a convex downward function of R; i.e., a function whose chords never lie below the function. This fact, of course, also follows from $\partial E(R, \mathbf{p})/\partial R$ decreasing with ρ and thus increasing with R.

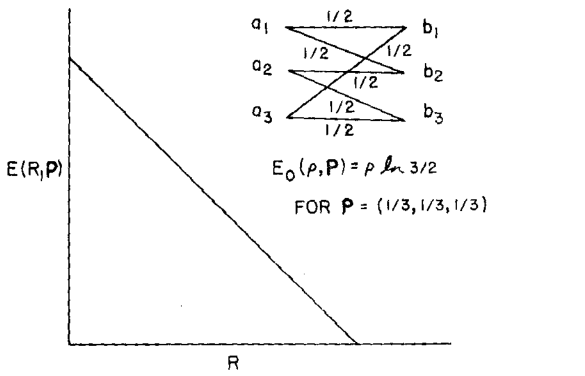


Fig. 4. Exponent, rate curve for channel with $\partial^2 E_0(\rho, \mathbf{p})/\partial\rho^2 = 0$.

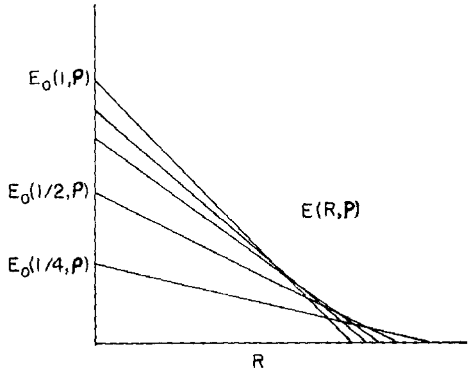


Fig. 5. Exponent, rate curve as envelope of straight lines.

All of the results in this section thus far have dealt with the function $E(R, \mathbf{p})$ defined in (31). The function, $E(R)$, in (22) can be expressed as

$$E(R) = \max_{\mathbf{p}} E(R, \mathbf{p}) \tag{38}$$

where the maximization is over all K-dimensional probability vectors, $\mathbf{p}$. Thus $E(R)$ is the upper envelope of all of the $E(R, \mathbf{p})$ curves, and we have the following theorem.

Theorem 3

For every discrete memoryless channel, the function $E(R)$ is positive, continuous, and convex downward for all R in the range $0 \leq R < C$. Thus the error probability bound $P_e \leq \exp - NE(R)$ is an exponentially decreasing function of the block length for $0 \leq R < C$.

Proof: If $C = 0$, the theorem is trivially true. Otherwise, for the $\mathbf{p}$ that achieves capacity, we have shown that $E(R, \mathbf{p})$ is positive for $0 \leq R < C$, and thus $E(R)$ is positive in the same range. Also, for every probability vector, $\mathbf{p}$, we have shown that $E(R, \mathbf{p})$ is continuous and convex downward with a slope between 0 and -1, and therefore the upper envelope is continuous and convex downward.

One might further conjecture that $E(R)$ has a continuous slope, but this is not true, as we shall show later. $E(R, \mathbf{p})$ has a continuous slope for any $\mathbf{p}$, but the $\mathbf{p}$ that maximizes $E(R, \mathbf{p})$ can change with R and this can lead to discontinuities in the slope of $E(R)$.

We next turn our attention to the actual maximization of $E(R, \mathbf{p})$ over $\mathbf{p}$. We may rewrite (22) as

$$E(R) = \max_{0 \leq \rho \leq 1} [- \rho R + \max_{\mathbf{p}} E_0(\rho, \mathbf{p})] \qquad (39)$$

Now define

$$F(\rho, \mathbf{p}) = \sum_i \left(\sum_k p_k P_{ik}^{1/(1+\rho)} \right)^{1+\rho} \qquad (40)$$

From (20), $E_0(\rho, \mathbf{p}) = -\ln F(\rho, \mathbf{p})$, so that minimizing $F(\rho, \mathbf{p})$ over $\mathbf{p}$ will maximize $E_0(\rho, \mathbf{p})$.

Theorem 4

$F(\rho, \mathbf{p})$, as given by (40), is a convex downward function of $\mathbf{p}$ over the region in which $\mathbf{p} = (p_1, \cdots, p_k)$ is a probability vector. Necessary and sufficient conditions on the vector (or vectors) $\mathbf{p}$ that minimize $F(\rho, \mathbf{p})$ [and maximize $E_0(\rho, \mathbf{p})$] are

$$\sum_i P_{ik}^{1/(1+\rho)} \alpha_i^\rho \geq \sum_i \alpha_i^{1+\rho} \qquad \text{for all } k \qquad (41)$$

with equality if $p_k \neq 0$, where $\alpha_i = \sum_k p_k P_{ik}^{1/(1+\rho)}$

This theorem is proved in the Appendix. If all the p_k are positive, (41) is simply the result of applying a Lagrange multiplier to minimize $F(\rho, \mathbf{p})$ subject to $\sum p_k = 1$. As shown in the Appendix, the same technique can be used to get the necessary and sufficient conditions on $\mathbf{p}$ to maximize $I(\mathbf{p})$. The result, which has also been derived independently by Eisenberg, is

$$\sum_i P_{jk} \ln \frac{P_{jk}}{\sum_i p_i P_{ji}} \leq I(\mathbf{p}) \qquad \text{for all } k \qquad (42)$$

with equality if $p_k \neq 0$.

Neither (41) nor (42) is very useful in finding the maximum of $E_0(\rho, \mathbf{p})$ or $I(\mathbf{p})$, but both are useful theoretical tools and are useful in verifying that a hypothesized solution is indeed a solution. For channels of any complexity, $E_0(\rho, \mathbf{p})$ and $I(\mathbf{p})$ can usually be maximized most easily by numerical techniques.

Given the maximization of $E_0(\rho, \mathbf{p})$ over $\mathbf{p}$, we can find the function $E(R)$ in any of three ways. First, from (39), $E(R)$ is the upper envelope of the family of straight lines given by

$$- \rho R + \max_{\mathbf{p}} E_0(\rho, \mathbf{p}) \qquad 0 \leq \rho \leq 1 \qquad (43)$$

Also, we can plot $\max_{\mathbf{p}} E_0(\rho, \mathbf{p})$ as a function of ρ, and use the graphical technique of Fig. 2 to find $E(R)$.

Finally, we can use the parametric equations, (34) and (35), and for each ρ use the $\mathbf{p}$ that maximizes $E_0(\rho, \mathbf{p})$. To see that this generates the curved portion of $E(R)$, let ρ_0 be a fixed value of ρ, $0 < \rho_0 < 1$, and let $\mathbf{p}_0$ maximize $E_0(\rho_0, \mathbf{p})$. We have already seen that the only point on the straight line $-\rho_0 R + E_0(\rho_0, \mathbf{p}_0)$ that lies on the curve $E(R, \mathbf{p}_0)$, and thus that can lie on $E(R)$, is that given by (34) and (35). Since the straight lines $-\rho R + \max_{\mathbf{p}} E_0(\rho, \mathbf{p})$ generate all points on the $E(R)$ curve, we see that (34)–(36), with $E_0(\rho, \mathbf{p})$ maximized over $\mathbf{p}$, generate all points on the $E(R)$ curve. These parametric equations can, under pathological conditions, also lead to some points not on the $E(R)$ curve. To see this, consider the channel of Fig. 6. From (41), we can verify that for $\rho \leq 0.51$, $E_0(\rho, \mathbf{p})$ is maximized by $p_1 = p_2 = p_3 = p_4 = \frac{1}{4}$. For $\rho > 0.51$, $E_0(\rho, \mathbf{p})$ is maximized by $p_5 = p_6 = \frac{1}{2}$. The parametric equations are discontinuous at $\rho = 0.51$ where the input distribution suddenly changes. Figure 6 shows the $E(R)$ curve for this channel and the spurious points generated by (34) and (35).

	b_1	b_2	b_3	b_4
a_1	0.82	0.06	0.06	0.06
a_2	0.06	0.82	0.06	0.06
a_3	0.06	0.06	0.82	0.06
a_4	0.06	0.06	0.06	0.82
a_5	0.49	0.49	0.01	0.01
a_6	0.01	0.01	0.49	0.49

TRANSITION PROBABILITY MATRIX

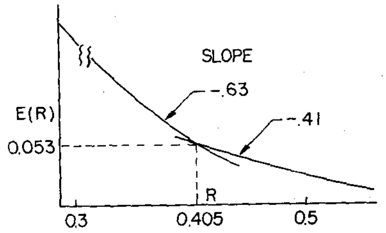


Fig. 6. A pathological channel.

The preceding discussion has described in detail the exponent $E(R)$ controlling the upper bound to error probability described in Section I. It can be shown that the exponent $E_L(R)$ controlling the lower bound to error probability in (1) is given by

$$E_L(R) = \underset{0<\rho<\infty}{\text{g.l.b.}} [- \rho R + \max_{\mathbf{p}} E_0(\rho, \mathbf{p})] \qquad (44)$$

Comparing (39) and (44), we see that the only difference is in the range in which ρ is to be maximized. Interpreting $E(R)$ and $E_L(R)$ as the upper envelopes of a family of straight lines of slope $-\rho$, we see that $E(R) = E_L(R)$ for $R_{crit} \leq R < C$, where the critical rate R_{crit} is defined as the g.l.b. of R values for which the slope of $E_L(R)$ is not less than -1. This is a nonzero range of R unless, for the $\mathbf{p}$ that maximizes $E_0(\rho, \mathbf{p})$, we have $\partial^2 E_0(\rho, \mathbf{p})/\partial \rho^2 = 0$ for $0 < \rho \leq 1$; the channel in Fig. 5 is such a channel.

IV. Examples and Applications

Binary Symmetric Channel

A binary symmetric channel has 2 inputs, 2 outputs, and transition probabilities $P_{12} = P_{21} = q$, and $P_{11} =$

$P_{22} = 1 - q$. Thus q is the probability of error on the channel with no coding. Clearly, the input probability vector that maximizes $E_0(\rho, \mathbf{p})$ is $p_1 = p_2 = \frac{1}{2}$. [Formally this can be shown by substitution in (41).] For this choice of $\mathbf{p}$,

$$E_0(\rho, \mathbf{p}) = -\ln \sum_{j=1}^{2} \left(\sum_{k=1}^{2} p_k P_{jk}^{1/(1+\rho)} \right)^{1+\rho}$$

$$= \rho \ln 2 - (1 + \rho) \ln [q^{1/(1+\rho)} + (1 - q)^{1/(1+\rho)}] \tag{45}$$

We now differentiate (45) and evaluate the parametric expressions for exponent and rate, (34) and (35). After some manipulation, we obtain

$$R = \ln 2 - H(q_\rho) \tag{46}$$

$$H(q_\rho) = -q_\rho \ln q_\rho - (1 - q_\rho) \ln (1 - q_\rho) \tag{47}$$

$$E(R, \mathbf{p}) = q_\rho \ln \frac{q_\rho}{q} + (1 - q_\rho) \ln \frac{1 - q_\rho}{1 - q} \tag{48}$$

where

$$q_\rho = \frac{q^{1/(1+\rho)}}{q^{1/(1+\rho)} + (1 - q)^{1/(1+\rho)}} \tag{49}$$

These equations are valid for $0 \leq \rho \leq 1$, or for $\ln 2 - [H\sqrt{q}/(\sqrt{q} + \sqrt{1 - q})] \leq R \leq C$. For rates below this, we have (36), which becomes

$$E(R, \mathbf{p}) = \ln 2 - 2 \ln (\sqrt{q} + \sqrt{1 - q}) - R \tag{50}$$

Except for the lack of a coefficient, $P_e \leq e^{-NE(R,\mathbf{p})}$ [where $E(R, \mathbf{p})$ is given by (46), (48), and (50)] is the random coding bound to error probability on the binary symmetric channel, first derived by Elias [6].

Very Noisy Channels

In this section, we shall consider channels that are very noisy in the sense that the probability of receiving a given output is almost independent of the input. We shall see that a universal exponent, rate curve exists for these channels in the limit. It will be assumed that the channel is discrete and memoryless, although the result can be easily extended to continuous channels. Let $q_1, \cdots, q_J$ be a set of probabilities defined on the channel outputs, and define ϵ_{jk} by

$$P_{jk} = q_j(1 + \epsilon_{jk}) \tag{51}$$

We assume that $|\epsilon_{jk}| \ll 1$ for all j, k. Note that if (51) is multiplied by p_k and summed over k, we get

$$\sum_j q_j \epsilon_{jk} = 0 \qquad \text{for all } k \tag{52}$$

We now compute $E_0(\rho, \mathbf{p})$ for this channel:

$$E_0(\rho, \mathbf{p}) = -\ln \sum_j \left[\sum_k p_k q_j^{1/(1+\rho)} (1 + \epsilon_{jk})^{1/(1+\rho)} \right]^{1+\rho} \tag{53}$$

Expanding $(1 + \epsilon_{jk})^{1/(1+\rho)}$ in a power series in ϵ_{jk}, and dropping terms of higher order than the second, we get

$$E_0(\rho, \mathbf{p})$$

$$\approx -\ln \sum_j q_j \left[\sum_k p_k \left(1 + \frac{\epsilon_{jk}}{1 + \rho} - \frac{\rho \epsilon_{jk}^2}{2(1 + \rho)^2} \right) \right]^{1+\rho} \tag{54}$$

The bracketed term to the $(1 + \rho)$ power in (54) may be again expanded as a power series in the ϵ_{jk} to give

$$E_0(\rho, \mathbf{p}) \approx -\ln \sum_j q_j \left[1 + \sum_k p_k \epsilon_{jk} \right.$$

$$\left. - \frac{\rho}{2(1 + \rho)} \sum_k p_k \epsilon_{jk}^2 + \frac{\rho}{2(1 + \rho)} \left(\sum_k p_k \epsilon_{jk} \right)^2 \right] \tag{55}$$

Using (52), this becomes

$$E_0(\rho, \mathbf{p}) \approx -\ln \left\{ 1 - \frac{\rho}{2(1 + \rho)} \right.$$

$$\left. \cdot \sum_j q_j \left[\sum_k p_k \epsilon_{jk}^2 - \left(\sum_k p_k \epsilon_{jk} \right)^2 \right] \right\} \tag{56}$$

Finally, expanding (56) and dropping terms of higher than second order in ϵ_{jk}, we have

$$E_0(\rho, \mathbf{p}) \approx \frac{\rho}{1 + \rho} f(\mathbf{p}) \tag{57}$$

where the constant $f(\mathbf{p})$ is given by

$$f(\mathbf{p}) = \frac{1}{2} \sum_j q_j \left[\sum_k p_k \epsilon_{jk}^2 - \left(\sum_k p_k \epsilon_{jk} \right)^2 \right] \tag{58}$$

If we take the mutual information, $I(\mathbf{p})$, use (51) for the transition probabilities, and expand $I(\mathbf{p})$ as a power series in the ϵ_{jk}, dropping terms of higher than second order, we get $f(\mathbf{p})$. Thus channel capacity C is given approximately by

$$C \approx \max_{\mathbf{p}} f(\mathbf{p}) \tag{59}$$

$$\max_{\mathbf{p}} E_0(\rho, \mathbf{p}) \approx \frac{\rho}{1 + \rho} C \tag{60}$$

We can now solve explicitly for ρ to find $E(R) = \max_{0<\rho\leq 1} [-\rho R + \max_{\mathbf{p}} E_0(\rho, \mathbf{p})]$. The solution is

$$P_e \leq e^{-NE(R)}$$

$$E(R) \approx (\sqrt{C} - \sqrt{R})^2 \qquad R \geq \frac{C}{4} \tag{61}$$

$$E(R) \approx \frac{C}{2} - R \qquad R < \frac{C}{4} \tag{62}$$

It is to be observed that the exponent rate curve given by (61) and (62) is identical to that for orthogonal signals in white Gaussian noise [2].

Noisy channels, as defined in this way, were first considered by Reiffen [7], who showed that the exponent corresponding to zero rate was $C/2$.

Parallel Channels

Consider two discrete memoryless channels, the first with K inputs, J outputs, and transition probabilities P_{jk}, and the second with I inputs, L outputs, and transition probabilities Q_{li}. Let

$$E_0^*(\rho, \mathbf{p}) = -\ln \sum_{j=1}^{J} \left(\sum_{k=1}^{K} p_k P_{jk}^{1/(1+\rho)} \right)^{1+\rho}$$

$$E_0^{**}(\rho, \mathbf{q}) = -\ln \sum_{l=1}^{L} \left(\sum_{i=1}^{I} q_i Q_{li}^{1/(1+\rho)} \right)^{1+\rho}$$

where $\mathbf{p} = (p_1, \cdots, p_K)$ and $\mathbf{q} = (q_1, \cdots, q_I)$ represent arbitrary probability assignments on the inputs to the first and second channel, respectively.

Let us consider using these two channels in parallel; that is, in each unit of time, the transmitter sends one symbol over the first channel and one symbol over the second channel. If we consider this pair of channels as a single channel with KI inputs, JL outputs, and transition probabilities $P_{jk}Q_{li}$, then we can find an upper bound to the probability of error achievable through coding on the two channels together. The following theorem, the first half of which is due to R. M. Fano [8], relates the $E(R)$ curve for the parallel combination to the $E(R)$ curves for the individual channels.

Theorem 5

The minimum error probability achievable through coding can be upperbounded by

$$P_e \leq \exp - N[-\rho R + E_0(\rho, \mathbf{pq})] \qquad \text{for any} \quad \rho, 0 \leq \rho \leq 1 \tag{63}$$

where

$$E_0(\rho, \mathbf{pq}) = E_0^*(\rho, \mathbf{p}) + E_0^{**}(\rho, \mathbf{q}) \tag{64}$$

Furthermore, if we choose $\mathbf{p}$ and $\mathbf{q}$ to maximize $E_0^*(\rho, \mathbf{p})$ and $E_0^{**}(\rho, \mathbf{q})$, respectively, for a given ρ, then

$$E_0(\rho, \mathbf{pq}) = \max_{\mathbf{r}} E_0(\rho, \mathbf{r}) \tag{65}$$

where $\mathbf{r} = (r_{11}, r_{12}, \cdots, r_{1I}, r_{21}, \cdots, r_{2I}, \cdots, r_{KI})$ represents an arbitrary probability assignment to an input pair and $E_0(\rho, \mathbf{r})$ is the usual E_0 function [see (20)] as applied to the parallel channel combination.

Proof: Regarding the parallel channels as a single channel with input probability vector $\mathbf{r}$, we get

$$E_0(\rho, \mathbf{r}) = -\ln \sum_{j,l} \left[\sum_{k,i} r_{ki} (P_{jk}Q_{li})^{1/(1+\rho)} \right]^{1+\rho} \tag{66}$$

Now assume that the input probability assignment uses letters from the two channels independently; i.e., $r_{ki} = p_k q_i$, where $p_1, \cdots, p_K$ and $q_1, \cdots, q_I$ are probability assignments on the individual channels. Substituting $r_{ki} = p_k q_i$ in (66) and separating the sum on k and i, we get

$$E_0(\rho, \mathbf{r}) = -\ln \sum_{j,l} \left[\sum_k p_k P_{jk}^{1/(1+\rho)} \right]^{1+\rho} \cdot \left[\sum_i q_i q_{li}^{1/(1+\rho)} \right]^{1+\rho}$$

Separating the sum on j and l, we obtain

$$E_0(\rho, \mathbf{r}) = E_0^*(\rho, \mathbf{p}) + E_0^{**}(\rho, \mathbf{q}) \tag{67}$$

Next, we must show that $r_{ki} = p_k q_i$ maximizes $E_0(\rho, \mathbf{r})$ when $\mathbf{p}$ and $\mathbf{q}$ maximize E_0^* and E_0^{**}. We know from (41) that the $\mathbf{p}$ and $\mathbf{q}$ that maximize E_0^* and E_0^{**} must satisfy

$$\sum_j P_{jk}^{1/(1+\rho)} \alpha_j^\rho \geq \sum_j \alpha_j^{1+\rho} \text{ ; all } k \tag{68}$$

with equality if $p_k \neq 0$, where $\alpha_j = \sum_k p_k P_{jk}^{1/(1+p)}$, and

$$\sum_l Q_{li}^{1/(1+\rho)} \beta_l^\rho \geq \sum_l \beta_j^{1+\rho} \text{ ; all } i \tag{69}$$

with equality if $q_i \neq 0$, where $\beta_l = \sum_i q_i Q_{li}^{1/(1+p)}$.

Multiplying (68) and (69) together, we get

$$\sum_{j,l} (P_{jk}Q_{li})^{1/(1+\rho)} (\alpha_j \beta_l)^\rho \geq \sum_{j,l} (\alpha_j \beta_j)^{1+\rho} \tag{70}$$

with equality if $r_{ki} = p_k q_i \neq 0$.

We observe that (70) is the same as (41) applied to the parallel channel combination. Thus this choice of $\mathbf{r}$ maximizes $E_0(\rho, \mathbf{r})$, and the theorem is proven.

Theorem 5 has an interesting geometrical interpretation. Let $E(\rho)$ and $R(\rho)$ be the exponent and rate for the parallel combination, as parametrically related by (34) and (35) with the optimum choice of $\mathbf{r}$ for each ρ. Let $E^*(\rho)$, $R^*(\rho)$, $E^{**}(\rho)$, $R^{**}(\rho)$ be the equivalent quantities for the individual channels. From (64)

$$E(\rho) = E^*(\rho) + E^{**}(\rho) \tag{71}$$

$$R(\rho) = R^*(\rho) + R^{**}(\rho) \tag{72}$$

Thus the parallel combination is formed by vector addition of points of the same slope from the individual $E(\rho)$, $R(\rho)$ curves.

Theorem 5 clearly applies to any number of channels in parallel. If we consider a block code of length N as a single use of N identical parallel channels, then Theorem 5 justifies our choice of independent identically distributed symbols in the ensemble of codes.

V. Improvement of Bound for Low Rates

At low rates, the exponent $E(R)$ derived in Section III does not yield a tight bound on error probability. The exponent is so large at low rates that previously negligible effects such as assigning the same code word to two messages suddenly become important. In this section, we avoid this problem by expurgating those code words for which the error probability is high. Equation (7) gives a bound on error probability for a particular code when the mth word is transmitted. With $\rho = 1$, this is

$$P_{em} \leq \sum_{\mathbf{y} \epsilon Y_N} \sqrt{Pr(\mathbf{y}|\mathbf{x}_m)} \sum_{m' \neq m} \sqrt{Pr(\mathbf{y}|\mathbf{x}_{m'})} \tag{73}$$

This can be rewritten in the form

$$P_{em} \leq \sum_{m' \neq m} q(\mathbf{x}_m, \mathbf{x}_{m'}) \tag{74}$$

$$q(\mathbf{x}_m, \mathbf{x}_{m'}) = \sum_{\mathbf{y}} \sqrt{Pr(\mathbf{y}|\mathbf{x}_m)\, Pr(\mathbf{y}|\mathbf{x}_{m'})} \tag{75}$$

$$= \prod_{n=1}^{N} \sum_{j=1}^{J} \sqrt{Pr(b_j|x_{mn})\, Pr(b_j|x_{m'n})} \tag{76}$$

Equations (75) and (76) are equivalent through the usual arithmetic rule for the product of a sum, where $(b_1, \cdots, b_J)$ is the channel output alphabet. We define $-\ln q(\mathbf{x}_m, \mathbf{x}_{m'})$ as the discrepancy between $\mathbf{x}_m$ and $\mathbf{x}_{m'}$; this forms a useful generalization of Hamming distance on binary symmetric channels to general memoryless channels.

Since P_{em} in (72) is a function of a particular code, it is a random variable over an ensemble of codes. In this section we upperbound $Pr\ (P_{em} \geq B)$, where B is a number to be chosen later, and then expurgate code words for which $P_{em} \geq B$. Using a bar to represent an average over the ensemble of codes, we obtain

$$Pr(P_{em} \geq B) = \overline{\phi_m(\text{code})} \tag{77}$$

$$\phi_m(\text{code}) = \begin{cases} 1 \text{ } if\ P_{em} \geq B \\ 0 \text{ otherwise} \end{cases} \tag{78}$$

We upperbound ϕ_m by

$$\phi_m(\text{code}) \leq \sum_{m' \neq m} \frac{q(\mathbf{x}_m, \mathbf{x}_{m'})^s}{B^s} \qquad 0 < s \leq 1 \tag{79}$$

Equation (79) is obvious for $\phi_m = 0$. If $\phi_m = 1$ and $s = 1$, (79) follows from (78) and (74). Decreasing s increases all the terms in (79) that are less than 1, and if any term is greater than 1, (79) is valid anyway. Substituting (79) in (77), we have

$$Pr(P_{em} \geq B) \leq B^{-s} \sum_{m' \neq m} \overline{q(\mathbf{x}_m, \mathbf{x}_{m'})^s} \tag{80}$$

Let the letters of the code words in the ensemble of codes be chosen independently by using the probabilities $p_1, \cdots, p_K$ so that $Pr\ (\mathbf{x}_m) = \prod_{n=1}^{N} Pr(x_{mn})$, where $Pr\ (x_{mn}) = p_k$ for $x_{mn} = p_k$. Then using (76), we have

$$\overline{q(\mathbf{x}_m, \mathbf{x}_{m'})^s} = \sum_{\mathbf{x}_m, \mathbf{x}_{m'}} Pr(\mathbf{x}_m) Pr(\mathbf{x}_{m'})$$

$$\cdot \prod_{n=1}^{N} \left[\sum_{j=1}^{J} \sqrt{Pr(b_j|x_{mn})\, Pr(b_j|x_{m'n})} \right]^s \tag{81}$$

$$= \prod_{n=1}^{N} \sum_{k=1}^{K} \sum_{i=1}^{K} p_k p_i \left[\sum_{j=1}^{J} \sqrt{Pr(b_j|a_k) Pr(b_j|a_i)} \right]^s \tag{82}$$

Since (82) is independent of m and m', we can substitute it in (80) to get

$$Pr(P_{em} \geq B)$$

$$\leq (M-1)B^{-s} \left[\sum_{k=1}^{K} \sum_{i=1}^{K} p_k p_i \left(\sum_{j=1}^{J} \sqrt{P_{jk} P_{ji}} \right)^s \right]^N$$

$$\text{for any } s, \quad 0 < s \leq 1 \tag{83}$$

Now choose B so that the right-hand side of (83) is equal to $\frac{1}{2}$. Then

$$Pr(P_{em} \geq B) \leq 1/2$$

$$B = [2(M-1)]^{1/s} \left[\sum_{k,i} p_k p_i \left(\sum_{j} \sqrt{P_{jk} P_{ji}} \right)^s \right]^{N/s} \tag{84}$$

If we expurgate all code words in the ensemble for which $P_{em} \geq B$, where B is given by (84), the average number of code words remaining in a code is at least $M/2$, since the probability of expurgation is at most $\frac{1}{2}$. Thus there exists a code with $M' \geq M/2$ code words with the error probability for each code word bounded by

$$P_{em} < B < (4M')^{1/s} \left[\sum_{k,i} p_k p_i \left(\sum_{j} \sqrt{P_{jk} P_{ji}} \right)^s \right]^{N/s} \tag{85}$$

Note that removing a code word from a code cannot increase the error probability associated with any other code word. If we let $M' = e^{NR}$ and define $\rho = 1/s$, (85) can be written

$$P_{em} < \exp - N \left[-\rho R + E_x(\rho, \mathbf{p}) - \rho \frac{\ln 4}{N} \right]$$

$$\text{for any} \quad \rho \geq 1 \tag{86}$$

$$E_x(\rho, \mathbf{p}) = -\rho \ln \sum_{k,1} p_k p_i \left(\sum_{j} \sqrt{P_{jk} P_{ji}} \right)^{1/\rho} \tag{87}$$

We can summarize the preceding results in the following theorem.

Theorem 6

Consider a discrete memoryless channel with input alphabet $a_1, \cdots, a_K$, output alphabet $b_1, \cdots, b_J$, and transition probabilities $P_{jk} = Pr\ (b_j \mid a_k)$. Then for any block length N and any number of code words $M' = e^{NR}$, there exists a code such that, for all m, $1 \leq m \leq M'$, the probability of decoding error when the mth code word is transmitted is bounded by (86) and (87), where $\mathbf{p} = (p_1, \cdots, p_K)$ in (87) is an arbitrary probability vector.

The expurgation technique leading to Theorem 6 is somewhat similar to an earlier expurgation technique applied by Elias [6] to the binary symmetric channel and by Shannon [9] to the additive Gaussian noise channel. The final bound here is somewhat tighter than those bounds and, in fact, the difference between the exponent derived here and the earlier exponents is equal to the rate, R.

The interpretation of Theorem 6 is almost identical to that of Theorem 1. The exponent rate curve given by (86) is the upper envelope of a set of straight lines; the line corresponding to each value of $\rho \geq 1$ has slope $-\rho$ and intercept $E_x(\rho, \mathbf{p})$ on the E axis. The following theorem, which is proved in the Appendix, gives the properties of $E_x(\rho, \mathbf{p})$.

Theorem 7

Let P_{jk} be the transition probabilities of a discrete memoryless channel and let $\mathbf{p} = (p_1, \cdots, p_K)$ be a probability vector on the channel inputs. Assume that

$$I(\mathbf{p}) = \sum_{k,i} p_k P_{jk} \ln \frac{P_{jk}}{\sum_i p_i P_{ji}} \neq 0$$

Then for $\rho > 0$, $E_x(\rho, \mathbf{p})$ as given by (87) is strictly increasing with ρ. Also, $E_x(1, \mathbf{p}) = E_0(1, \mathbf{p})$, where E_0 is given by (20). Finally, $E_x(\rho, \mathbf{p})$ is strictly convex upward with ρ unless the channel is noiseless in the sense that for each pair of inputs, a_k and a_i, for which $p_k \neq 0$ and $p_i \neq 0$, we have either $P_{jk}P_{ji} = 0$ for all j or $P_{jk} = P_{ji}$ for all j.

This theorem can be used in exactly the same way as Theorem 2 to obtain a parametric form for the exponent, rate curve at low rates. Let

$$E(R, \mathbf{p}) = \max_{\rho} \left[-\rho R + E_x(\rho, \mathbf{p}) - \rho \frac{\ln 4}{N} \right] \tag{88}$$

Then, for R in the range

$$\lim_{\rho \to \infty} \frac{\partial E_x(\rho, \mathbf{p})}{\partial \rho} \leq R + \frac{\ln 4}{N} \leq \left. \frac{\partial E_x(\rho, \mathbf{p})}{\partial \rho} \right|_{\rho=1} \tag{89}$$

we have the parametric equations in ρ

$$\left. \begin{aligned} R + \frac{\ln 4}{N} &= \frac{\partial E_x(\rho, \mathbf{p})}{\partial \rho} \\ E(R, \mathbf{p}) &= -\rho \frac{\partial E_x(\rho, \mathbf{p})}{\partial \rho} + E_x(\rho, \mathbf{p}) \end{aligned} \right\} \tag{90}$$

If $E_x(\rho, \mathbf{p})$ is a strictly convex function of ρ, then (90) represents a convex downward curve with a continuous slope given by $-\rho$.

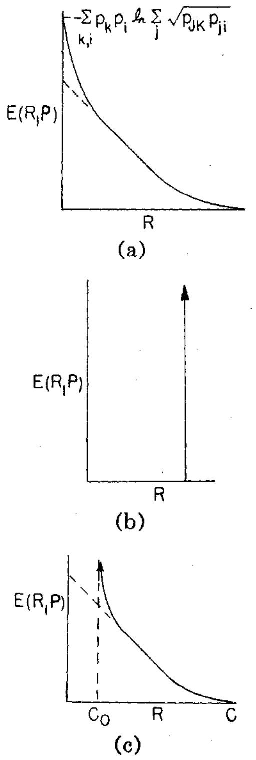
The smallest rate for which (90) is applicable is

$$\lim_{\rho \to \infty} \frac{\partial E_x(\rho, \mathbf{p})}{\partial \rho} = \lim_{\rho \to \infty} -\ln \sum_{k,i} p_k p_i \left(\sum_j \sqrt{P_{jk} P_{ji}} \right)^{1/\rho}$$
$$= -\ln \sum_{k,i} p_k p_i \phi_{ki} \tag{91}$$

where

$$\phi_{ki} = \begin{cases} 1 & \text{if } \sum_j P_{jk} P_{ji} \neq 0 \\ 0 & \text{if } \sum_j P_{jk} P_{ji} = 0 \end{cases}$$

If there are two inputs in use, k and i, for which there are no common outputs (i.e., for which $\sum_j P_{jk} P_{ji} = 0$), then the right-hand side of (91) is strictly positive. If $R + \ln 4/N$ is less than this quantity, then $E(R, \mathbf{p})$ is infinite. This can be seen most easily by regarding the $E(R, \mathbf{p})$, R curve as the upper envelope of straight lines of slope $-\rho$; the right-hand side of (91) is the limit of the R intercepts of these lines as the slope approaches $-\infty$. Shannon [10] has defined the zero error capacity of a channel as the greatest rate at which transmission is possible with no errors; the right-hand side of (91) thus gives a lower bound to zero error capacity. Fig. 7 shows the exponent, rate curves given by Theorem 6 for some typical channels.



(a)

(b)

(c)

Fig. 7. Typical exponent, rate curves obtained by using low-rate improvement. (a) Ordinary channel. (b) Noiseless channel. (c) Channel with zero error capacity.

If the channel is noiseless in the sense of Theorem 7, then it is not hard to see that $E(R, \mathbf{p})$, as given by (88), is infinite for $R + (\ln 4)/N < I(\mathbf{p})$. It is no great achievement to show that zero error probability is possible on noiseless channels below capacity, but it is satisfying to see that this result comes naturally out of the general formulation.

Very little can be said about the maximization of $E_x(\rho, \mathbf{p})$ over the input probability vector $\mathbf{p}$. It is possible for a number of local maxima to exist, and no general maximization techniques are known.

These low-rate results can be applied to parallel channels by the same procedure as used in Section IV. If the input probability vector $\mathbf{p}$ for the parallel channels chooses letters from the two channels independently, then $E_x(\rho, \mathbf{p})$ for the parallel combination is the sum of the $E_x(\rho, \mathbf{p})$ functions for the individual channels. Unfortunately, $E_x(\rho, \mathbf{p})$ is not always maximized by using the channels independently. An example of this, which is due to Shannon [10], is found by putting the channel in Fig. 8 in parallel with itself. The zero error capacity bound, $\lim_{\rho \to \infty} E_x(\rho, \mathbf{p})/\rho$, for the single channel is ln 2 achieved by using inputs 1 and 4 with equal probability in (91). For the parallel channels, (91) yields ln 5, achieved

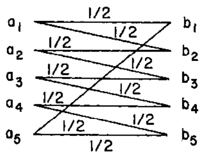


Fig. 8. Transition probabilities for a channel with zero error capacity.

by using the five pairs of inputs, (1, 1), (2, 3), (3, 5), (4, 2), (5, 4), with equal probability.

Theorem 6 yields a rather interesting result when applied to the binary symmetric channel. Letting q be the channel crossover probability and letting $\mathbf{p} = (\frac{1}{2}, \frac{1}{2})$, we rewrite (87)

$$E_x(\rho, \mathbf{p}) = -\rho \ln \{\tfrac{1}{2} + \tfrac{1}{2}[4q(1-q)]^{1/2\rho}\} \tag{92}$$

Using (92) in the parametric equations, (90), and going through some algebraic manipulation, we get

$$R + \frac{\ln 4}{N} = \ln 2 - H(\delta) \tag{93}$$

$$E(R, \mathbf{p}) = \frac{\delta}{2} \ln \frac{1}{4q(1-q)} \tag{94}$$

where the parameter δ is related to ρ by $\delta/(1-\delta) = [4q(1-q)]^{1/2\rho}$, and $H(\delta) = -\delta \ln \delta - (1-\delta) \ln (1-\delta)$. Equations (93) and (94) are valid for $\delta \geq \sqrt{4q(1-q)} / (1 + \sqrt{4q(1-q)})$.

For large N, δ in (93) approaches $D_{\min}/N$, where $D_{\min}$ is the Gilbert bound [11] on minimum distance for a binary code of rate R. The exponent given by (94) turns out to be the same as the exponent for probability of confusion between two code words at the Gilbert distance from each other. This result has also been established for parity-check codes [12].

VI. Continuous Channels and Input Constraints

A time-discrete amplitude-continuous channel is a channel whose input and output alphabets are the set of real numbers. It is usually necessary or convenient to impose a constraint on the code words of such channels to reflect the physical power limitations of the transmitter. Thus, before discussing continuous channels, we discuss the effects of constraints on discrete channels and then generalize the results to continuous channels.

It is possible to include constraints in Theorem 1 by choosing the code ensemble in such a way that the average code word will satisfy the constraint. There are two difficulties with such a procedure. One is the mathematical technicality that not all of the words satisfy the constraint. The other, more important, difficulty is that those code words that satisfy the constraint with a considerable amount to spare sometimes have such a high error probability that the upper bound given by Theorem 1 is not exponentially the tightest bound that can be derived.

In this section, we modify Theorem 1 to get the best exponential bound for discrete channels with input constraints. Then we extend the bound to the continuous channel, and, finally, we use the additive Gaussian noise channel as an example.

Let $f_1 = f(a_1), \cdots, f_K = f(a_K)$ be a real-valued (positive and negative) function of the input letters, $a_1, \cdots, a_K$. We wish to consider codes for which each code word, $\mathbf{x} = (x_1, \cdots, x_N)$, is constrained to satisfy

$$\sum_{n=1}^{N} f(x_n) \leq 0 \tag{95}$$

If the input letters are voltage levels and if $f(a_k) = a_k^2 - S_0$, then (95) is a power constraint, constraining each code word to an average power of S_0 per letter. Let $\mathbf{p} = (p_1, \cdots, p_K)$ be a probability vector whose components satisfy

$$\sum_{k=1}^{K} p_k f_k \leq 0 \tag{96}$$

We now define an ensemble of codes in which the probability of a code word $P(\mathbf{x})$ is the conditional probability of picking the letters according to $\mathbf{p}$, given that the constraint $-\delta \leq \sum_{n=1}^{N} f(x_n) \leq 0$, where δ is a number to be chosen later, is satisfied. Mathematically,

$$P(\mathbf{x}) = q^{-1}\phi(\mathbf{x}) \prod_{n=1}^{N} p(x_n) \tag{97}$$

$$\phi(\mathbf{x}) = \begin{cases} 1 & \text{if } -\delta \leq \sum_n f(x_n) \leq 0 \\ 0 & \text{otherwise} \end{cases} \tag{98}$$

$$q = \sum_{\mathbf{x}} \phi(\mathbf{x}) \prod_{n=1}^{N} p(x_n) \tag{99}$$

where $p(x_n) = p_k$ for $x_n = a_k$. We can think of q as a normalizing factor that makes $P(\mathbf{x})$ sum to 1.

We now substitute (99) in (11), remembering that (11) is valid for any ensemble of codes.

$$P_{em} \leq (M-1)^{\rho} \sum_{\mathbf{y}} \left[\sum_{\mathbf{x}} q^{-1}\phi(\mathbf{x}) \cdot \prod_{n=1}^{N} p(x_n)\, Pr(\mathbf{y}|\mathbf{x})^{1/(1+\rho)} \right]^{1+\rho} \qquad 0 \leq \rho \leq 1 \tag{100}$$

Before simplifying (100), we upperbound $\phi(\mathbf{x})$.

$$\phi(\mathbf{x}) \leq \exp r\left[\sum_{n=1}^{N} f(x_n) + \delta \right] \quad \text{for} \quad r \geq 0 \tag{101}$$

Equation (101) is obviously valid for $\phi(\mathbf{x}) = 0$; for $\phi(\mathbf{x}) = 1$, we have $\sum_{n=1}^{N} f(x_n) + \delta \geq 0$, and (101) is still valid. The right-hand side of (101) is mathematically more tractable than the left, but still avoids large contributions to P_{em} from sequences for which $\sum_n f(x_n)$ is too small.

Substituting (101) in (100) and going through the same set of steps that were used from (11) to (20), we have proved the following theorem.

Theorem 8

Under the same conditions as Theorem 1, there exists a code in which each code word satisfies the constraint $\sum_{n=1}^{N} f(x_n) \leq 0$ and the probability of decoding error is bounded by

$$P_e \leq B \exp - N[E_0(\rho, \mathbf{p}, r) - \rho R] \tag{102}$$

$$E_0(\rho, \mathbf{p}, r) = - \ln \sum_{j=1}^{J} \left[\sum_{k=1}^{K} p_k P_{jk}^{1/(1+\rho)} e^{rf_k} \right]^{1+\rho} \tag{103}$$

$$B = \left(\frac{e^{r\delta}}{q} \right)^{1+\rho} \tag{104}$$

where q satisfies (99). Equations (102)–(104) are valid for any ρ, $0 \leq \rho \leq 1$, any $r \geq 0$, any $\delta > 0$, and any $\mathbf{p}$ satisfying $\sum p_k f_k \leq 0$.

We note that if $r = 0$, (103) is the same as (20) except for the coefficient B. If the $\mathbf{p}$ that maximizes $E_0(\rho, \mathbf{p})$ in (20) satisfies the constraint $\sum_{k=1}^{K} p_k f_k \leq 0$, we can set $r = 0$ and get the same exponential error behavior as in the unconstrained case. Under these circumstances, if we choose δ large enough, then q will approach $\frac{1}{2}$ with increasing N if $\sum_k p_k f_k = 0$ and will approach 1 for $\sum p_k f_k < 0$.

The more interesting application of Theorem 8 is to cases in which the $\mathbf{p}$ that maximizes $E_0(\rho, \mathbf{p})$ in (20) does not satisfy the constraint $\sum p_k f_k \leq 0$; it turns out in this case that $E_0(\rho, \mathbf{p}, r)$ is maximized by choosing $r > 0$.

The engineering approach to the maximization of $E_0(\rho, \mathbf{p}, r)$ over $\mathbf{p}$, r is to conclude that, since the unconstrained maximum is by hypothesis outside the constraint region, the constrained maximum is at the constraint boundary, $\sum_k p_k f_k = 0$. We can then find a stationary point to the quantity inside the logarithm in (104) by using Lagrange multipliers for the constraints $\sum_k p_k = 1$, $\sum_k p_k f_k = 0$. This procedure gives us

$$(1 + \rho) \sum_{j=1}^{J} \alpha_j^{\rho} P_{jk}^{1/(1+\rho)} e^{rf_k} + \lambda + \gamma f_k \geq 0 \quad \text{for all } k \tag{105}$$

with equality if $p_k \neq 0$.

$$\alpha_j = \sum_k p_k P_{jk}^{1/(1+\rho)} e^{rf_k} \tag{106}$$

The inequality in (105) is to account for maxima where some of the $p_k = 0$, as in Theorem 4. We also require a stationary point with respect to r, which gives us

$$(1 + \rho) \sum_j \alpha_j^{\rho} \sum_k p_k f_k P_{jk}^{1/(1+\rho)} e^{rf_k} = 0 \tag{107}$$

If we multiply (105) by p_k and sum over k, we find that $\lambda = -(1 + \rho) \sum_j \alpha_j^{1+\rho}$. If we multiply (105) by $p_k f_k$, sum over k, and compare with (107), we find that $\gamma = 0$. Combining these results, we obtain

$$\sum_j \alpha_j^{\rho} P_{jk}^{1/(1+\rho)} e^{rf_k} \geq \sum_j \alpha_j^{1+\rho} \text{ ; for all } k \tag{108}$$

with equality if $p_k \neq 0$.

It can be shown, although the proof is more involved than that of Theorem 4, that (108) and the constraints $\sum_k p_k = 1$ and $\sum_k p_k f_k = 0$ are necessary and sufficient conditions on the r and $\mathbf{p}$ that maximize $E_0(\rho, \mathbf{p}, r)$ when the unconstrained maximum does not satisfy $\sum p_k f_k \leq 0$. When $\mathbf{p}$ and r are maximized in this way, and (102) is maximized over ρ, it can then be shown that for $R \geq R_{\text{crit}}$ (102) has the true exponential behavior with N of the best code of block length N satisfying the given constraint.

The quantity B in (102) and (103) is difficult to bound, but it can be estimated quite easily for large N from the central-limit theorem. Let $S = \sum_{n=1}^{N} \xi_n$, where the ξ_n are independent and $\xi_n = f_k$ with probability p_k. Then $q = Pr\,[-\delta \leq S \leq 0]$, and it follows from the central-limit theorem[7] that, for fixed δ,

$$\lim_{N \to \infty} \sqrt{N}\, q = \frac{\delta}{\sqrt{2\pi}\, \sigma_f} \tag{109}$$

$$\sigma_f^2 = \sum_k p_k f_k^2 \tag{110}$$

Using (109) in (103), we see that $e^{r\delta}/q$ is approximately minimized by choosing $\delta = 1/r$, with the result

$$\frac{e^{r\delta}}{q} \approx \sqrt{2\pi N}\, \sigma_f e r \tag{111}$$

Here, $\approx$ means that the ratio of the two sides approaches 1 as $N \to \infty$. If the ξ_n are lattice distributions,[7] then δ must be a multiple of the span, and (111) is not valid, although B is still proportional to $N^{(1+\rho)/2}$.

Input Constraints at Low Rates

At low rates, the bound given by (102) and (103) can be improved upon in the same way as Theorem 6 improved upon Theorem 1. In order to do this, we simply choose $Pr\,(\mathbf{x}_m)$ and $Pr\,(\mathbf{x}_{m'})$ in (81) to be given by (97). Applying the bound in (101) to (97), and substituting in (81), we can simplify the expression to get

$$\overline{q(\mathbf{x}_m, \mathbf{x}_{m'})^s} = \frac{e^{2r\delta}}{q^2} \left[\sum_{k=1}^{K} \sum_{i=1}^{K} p_k p_i e^{r(f_k + f_i)} \left(\sum_{j=1}^{J} \sqrt{P_{jk} P_{ji}} \right)^s \right]^N \tag{112}$$

Using (112) in place of (82) and carrying through the same argument used in going from (82) to (87), we get the following theorem.

Theorem 9

Under the same conditions as in Theorem 6, there exists a code for which each code word satisfies both $\sum_n f(x_n) \leq 0$ and

[7] If the ξ_n have a nonlattice distribution, (109) follows after a little algebra from Theorem 2, page 210, of Gnedenko and Kolmogorov [13]. If the ξ_n have a lattice distribution, (109) follows from the theorem on page 233, Gnedenko and Kolmogorov [13]. (A lattice distribution is a distribution in which the allowable values of ξ_n can be written in the form $d_k = h \cdot j(k) + a$, where a and h are independent of k and $j(k)$ is an integer for each k. The largest h satisfying this equation is the span of the distribution.) For nonlattice distributions, ξ_n must have a third absolute moment; this is trivial for finite input alphabets and sufficiently general for the continuous inputs that we wish to consider.

$$P_{em} < \exp - N\left\{E_x(\rho, \mathbf{p}, r,) - \rho\left[R + \frac{2}{N} \ln \frac{2e^{r\delta}}{q}\right]\right\} \quad (113)$$

$$E_x(\rho, \mathbf{p}, r) = - \rho \ln \sum_{k,i} p_k p_i e^{r(f_k + f_i)} \left(\sum_j \sqrt{P_{jk} P_{ji}} \right)^{1/\rho} \quad (114)$$

for any $\rho \geq 1$, $r \geq 0$, $\delta > 0$, and $\mathbf{p}$ satisfying $\sum_k p_k f_k \leq 0$. For $\sum_k p_k f_k = 0$, $e^{r\delta}/q$ is given by (109)–(111).

Continuous Channels

Consider a channel in which the input and output alphabets are the set of real numbers. Let $P(y \mid x)$ be the probability density of receiving y when x is transmitted. Let $p(x)$ be an arbitrary probability density on the channel inputs, and let $f(x)$ be an arbitrary real function of the channel inputs; assume that each code word is constrained to satisfy $\sum_{n=1}^{N} f(x_n) \leq 0$, and assume that $\int_{-\infty}^{\infty} p(x) f(x)\, dx = 0$.

Let the input space be divided into K intervals and the output space be divided in J intervals. For each k, let a_k be a point in the kth input interval, and let p_k be the integral of $p(x)$ over that interval. Let P_{jk} be the integral of $P(y \mid a_k)$ over the jth output interval. Then Theorems 8 and 9 can be applied to this quantized channel. By letting K and J approach infinity in such a way that the interval around each point approaches 0, the sums over k and j in Theorems 8 and 9 become Riemann integrals, and the bounds are still valid if the integrals exist.[8] Thus we have proved the following theorem.

Theorem 10

Let $P(y \mid x)$ be the transition probability density of an amplitude-continuous channel and assume that each code word is constrained to satisfy $\sum_{n=1}^{N} f(x_n) \leq 0$. Then for any block length N, any number of code words, $M = e^{NR}$, and any probability distribution on the use of the code words, there exists a code for which

$$P_e \leq B \exp\left[- N\{E_0(\rho, \mathbf{p}, r) - \rho R\}\right] \quad (115)$$

$$E_0(\rho, \mathbf{p}, r) = - \ln \int_{-\infty}^{\infty} \left[\int_{-\infty}^{\infty} p(x) P(y|x)^{1/(1+\rho)} e^{rf(x)} dx \right]^{1+\rho} \mathrm{dy} \quad (116)$$

$$B = \left(\frac{e^{r\delta}}{q}\right)^{1+\rho} \quad \text{for any } \rho, \quad 0 \leq \rho \leq 1 \quad (117)$$

Also, for any $\rho \geq 1$, we have for each code word

$$P_{em} < \exp - N\left\{E_x(\rho, \mathbf{p}, r) - \rho \left[R + \frac{2}{N} \ln \frac{2e^{r\delta}}{q}\right]\right\} \quad (118)$$

$$E_x(\rho, \mathbf{p}, r) = - \rho \ln \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} p(x) p(x') e^{rf(x) + rf(x')} \left(\int_{-\infty}^{\infty} \sqrt{P(y|x) P(y|x')}\, \mathrm{dy} \right)^{1/\rho} \mathrm{dx\, dx'} \quad (119)$$

Equations (115)–(119) are valid if the Riemann integrals exist for any $r \geq 0$, $\delta > 0$, and $p(x)$ satisfying $\int_{-\infty}^{\infty} p(x) f(x)\, dx \leq 0$. If $\int p(x) f(x)\, dx = 0$ and $\int p(x)\, |f(x)|^3\, dx < \infty$, then $e^{r\delta}/q \approx \sqrt{2\pi N} \sigma_f r e$ [see (111)].

In the absence of any input constraint, (115)–(119) still can be applied by setting $r = 0$, and $q = 1$.

Additive Gaussian Noise

As an example of the use of (115)–(119), we consider a time-discrete, amplitude-continuous, additive Gaussian noise channel. For such a channel, when $\mathbf{x}_m = (x_{m1}, \cdots, x_{mN})$ is transmitted, the received sequence, $\mathbf{y}$, can be represented as $(x_{m1} + z_1, \cdots, x_{mN} + z_N)$ when the z_n are Gaussian random variables, statistically independent of each other and of the input. We can assume without loss of generality that the scales of x and y are chosen so that each z_n has mean 0 and unit variance. Thus

$$P(y|x) = \frac{1}{\sqrt{2\pi}} e^{-(y-x)2/2} \quad (120)$$

We assume that each code word is power-constrained to satisfy

$$\sum_{n=1}^{N} x_{mn}^2 \leq NA \quad (121)$$

or

$$\sum_{n=1}^{N} f(x_{mn}) \leq 0; \qquad f(x) = x^2 - A \quad (122)$$

The quantity A in (121) and (122) is the *power* SNR per degree of freedom. One's intuition at this point would suggest choosing $p(x)$ to be Gaussian with variance A, and it turns out that this choice of $p(x)$ with an appropriate r yields a stationary point of $E_0(\rho, \mathbf{p}, r)$. Thus

$$p(x) = \frac{1}{\sqrt{2\pi A}} e^{-x^2/2A} \quad (123)$$

If we substitute (120), (122), and (123) in (116), the integrations are straightforward, and we get

$$E_0(\rho, \mathbf{p}, r) = rA(1 + \rho) + 1/2 \ln(1 - 2rA) + \frac{\rho}{2} \ln\left(1 - 2rA + \frac{A}{1 + \rho}\right) \quad (124)$$

Making the substitution $\beta = 1 - 2rA$ in (124) for simplicity and maximizing (124) over β, we get

$$\beta = 1/2\left\{1 - \frac{A}{1 + \rho} + \sqrt{\left(1 - \frac{A}{1 + \rho}\right)^2 + \frac{4A}{(1 + \rho)^2}}\right\} \quad (125)$$

[8] For the details of this limiting argument, see Gallager [3], Section 8.

Using (124) to maximize (116) over ρ, we get

$$P_e \leq B \exp - NE(R) \tag{126}$$

where $E(R)$ is given by the parametric equations in ρ, $0 \leq \rho \leq 1$,

$$E(R) = \tfrac{1}{2} \ln \beta + \frac{(1+\rho)(1-\beta)}{2} \tag{127}$$

$$R = \tfrac{1}{2} \ln \left(\beta + \frac{A}{1+\rho}\right) \tag{128}$$

where, for each ρ, β is given by (125).

The constant B in (126) is given by (104) and (111), where δ_f, from (122), is $\sqrt{2}A$. Thus, as $N \to \infty$

$$B \approx \left[4\pi N A^2 \left(\frac{1-\beta}{2A}\right)^2 e^2\right]^{(1+\rho)/2} = [\pi N e^2 (1-\beta)^2]^{(1+\rho)/2} \tag{129}$$

Equations (127) and (128) are applicable for $0 \leq \rho \leq 1$, or by substituting (125) in (128), for

$$\frac{1}{2} \ln \frac{1}{2} \left\{1 + \frac{A}{2} + \sqrt{1 + \frac{A^2}{4}}\right\} \leq R \leq \tfrac{1}{2} \ln (1 + A) \tag{130}$$

The left-hand side of (130) is R_{crit} and the right-hand side is channel capacity. In this region, $E(R)$ is the same exponent, rate curve derived by Shannon,[9] and this is the region in which Shannon's upper and lower bound exponent agree. Shannon's coefficient, however, is considerably tighter than the one given here.

In order to get the low-rate expurgated bound on error probability, we substitute (120), (122), and (123) in (119). After a straightforward integration, we get

$$E_x(\rho, \mathbf{p}, r) = 2r\rho A + \frac{\rho}{2} \ln (1 - 2rA) + \frac{\rho}{2} \ln \left(1 - 2rA + \frac{A}{2\rho}\right) \tag{131}$$

Letting $\beta_x = 1 - 2rA$, we find that $E_x(\rho, \mathbf{p}, r)$ is maximized by

$$\beta_x = \frac{1}{2}\left[1 - \frac{A}{2\rho} + \sqrt{1 + \frac{A^2}{4\rho^2}}\right] \tag{132}$$

Finally, optimizing (118) over ρ, we find

$$P_{em} < \exp - NE(R)$$

where $E(R)$ is given by the parametric equations for $\rho \geq 1$,

$$E(R) = \rho(1 - \beta_x)$$

$$R = \tfrac{1}{2} \ln \left(\beta_x + \frac{A}{4\rho}\right) - \frac{2}{N} \ln \frac{2e^{r\delta}}{q} \tag{133}$$

Here, as before, for N large

$$\frac{e^{r\delta}}{q} \approx \sqrt{\pi N}\, e(1 - \beta_x) \tag{134}$$

If we let

$$R' = R + \frac{2}{N} \ln \frac{2e^{r\delta}}{q} \tag{135}$$

we can solve (132)–(134) explicitly to get

$$E(R) = \frac{A}{4}\left(1 - \sqrt{1 - e^{-2R'}}\right) \tag{136}$$

for

$$R' \leq \frac{1}{2} \ln \left(\frac{1}{2} + \frac{1}{2}\sqrt{1 + \frac{A^2}{4}}\right) \tag{137}$$

The exponent given by (136) is larger than the low-rate exponent given by Shannon [9], the difference being equal to R'.

For rates between those specified by (130) and (137), we can use either (124) or (131) with $\rho = 1$. Either way, we get

$$P_e < B \exp - N\left[(1 - \beta) + \frac{1}{2} \ln \left(\beta + \frac{A}{4} - R\right)\right] \tag{138}$$

$$\beta = \frac{1}{2}\left[1 - \frac{A}{2} + \sqrt{1 + \frac{A^2}{4}}\right] \tag{139}$$

Figure 9 shows the $E(R)$ curve given by these equations for various SNR's.

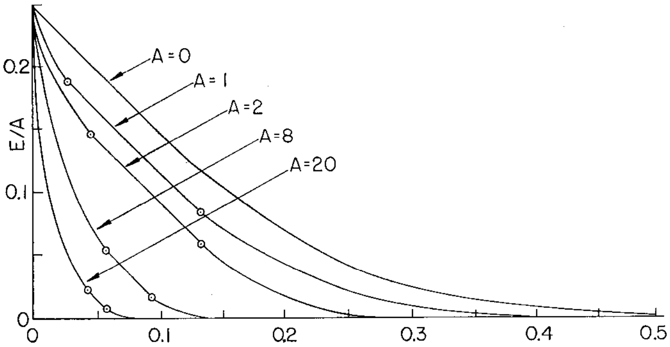


Fig. 9. Exponent, rate curve for additive Gaussian noise. A, power SNR.

Appendix

Both Theorems 2 and 7 require the following lemma in their proofs:

Lemma

Let $a_1, \cdots, a_L$ be a set of non-negative numbers and let $q_1, \cdots, q_L$ be a set of probabilities. Then

$$f(x) = \ln \left(\sum_l q_l a_l^{1/x}\right)^x \tag{140}$$

is nonincreasing with $x > 0$ and is strictly decreasing unless the a_l for which $q_l \neq 0$ are all equal. Also, $f(x)$

[9] The equivalence of (128) and (129) to Shannon's [9] equations (5) and (11) is seen only after a certain amount of algebra. The correspondence between the various parameters is as follows: we put Shannon's quantities on the right and use A_s for Shannon's A:

$$A = A_s^2 \quad \rho = \frac{A_s G(\theta_1) \sin^2 \theta_1}{\cos \theta_1} - 1\,; \beta = \frac{1}{[G(\theta_1)]^2 \sin^2 \theta_1}$$

is convex downward for $x > 0$ and is strictly convex downward unless all the nonzero a_l for which $q_l \neq 0$ are equal.

Proof: It is a well-known property of weighted means (see Hardy, et al. [14]) that $(\sum_l q_l a_l^r)^{1/r}$ is a nondecreasing function of r for $r > 0$ and is strictly increasing unless the a_l for which $q_l \neq 0$ are all equal. Let $x = 1/r$; this implies that $f(x)$ is nonincreasing or strictly decreasing with $x > 0$. Another property of weighted means[10] stemming from Holder's inequality is that if r and t are unequal positive numbers, θ satisfies $0 < \theta < 1$, and $s = \theta r + (1 - \theta)t$, then

$$\sum_l q_l a_l^s \leq \Big(\sum_l q_l a_l^r\Big)^{\theta}\Big(\sum q_l a_l^t\Big)^{1-\theta} \tag{141}$$

with equality only if all of the nonzero a_l for which $q_l \neq 0$ are equal. Let λ be defined by

$$\begin{aligned} \lambda &= \frac{r\theta}{r\theta + t(1-\theta)} \\ \frac{1}{s} &= \frac{\lambda}{r} + \frac{1-\lambda}{t} \end{aligned} \tag{142}$$

Substituting (142) in (141) and taking the $1/s$ power of each side, we get

$$\Big(\sum_l q_l a_l^s\Big)^{1/s} \leq \Big(\sum q_l a_l^r\Big)^{\lambda/r}\Big(\sum q_l a_l^t\Big)^{(1-\lambda)/t} \tag{143}$$

Taking the logarithm of both sides of (143) and interpreting $1/r$ and $1/t$ as two different values of x, we find that $f(x)$ is convex downward with strict convexity under the stated conditions.

Proof of Theorem 2:[11]

$$E_0(\rho, \mathbf{p}) = -\ln \sum_{j=1}^{J}\Big(\sum_{k=1}^{K} p_k P_{jk}^{1/(1+\rho)}\Big)^{1+\rho}$$

From the lemma, $(\sum_k p_k P_{jk}^{1/(1+\rho)})^{1+\rho}$ is nonincreasing with ρ. Since $I(\mathbf{p}) \neq 0$ by assumption, there is at least one j for which P_{jk} changes with k for $p_k \neq 0$; for that j, $(\sum_k p_k P_{jk}^{1/(1+\rho)})^{1+\rho}$ is strictly decreasing, and thus $E_0(\rho, \mathbf{p})$ is strictly increasing with ρ. From direct calculation we see that $E_0(0, \mathbf{p}) = 0$ and consequently it follows that for $\rho > 0$ $E_0(\rho, \mathbf{p}) > 0$ and $\partial E_0(\rho, \mathbf{p})/\partial\rho > 0$. By direct differentiation, it is also seen that $\partial E_0/\partial\rho\,|_{\rho=0} = I(\mathbf{p})$. Next, let ρ_1 and ρ_2 be unequal positive numbers, let λ satisfy $0 < \lambda < 1$, and let $\rho_3 = \lambda\rho_1 + (1 - \lambda)\rho_2$. From the lemma,

$$\begin{aligned} &\Big(\sum_k p_k P_{jk}^{1/(1+\rho_3)}\Big)^{1+\rho_3} \\ &\quad\leq \Big(\sum_k p_k P_{jk}^{1/(1+\rho_1)}\Big)^{\lambda(1+\rho_1)}\Big(\sum_k p_k P_{jk}^{1/(1+\rho_2)}\Big)^{(1-\lambda)(1+\rho_2)} \end{aligned} \tag{144}$$

We now apply Holder's inequality,[12] which states that if a_j and b_j are sets of non-negative numbers, then

$$\sum_j a_j b_j \leq \Big(\sum_j a_j^{1/\lambda}\Big)^{\lambda}\Big(\sum_j b_j^{1/(1-\lambda)}\Big)^{1-\lambda} \tag{145}$$

with equality only if the a_j and b_j are proportional. Summing (144) over j, letting a_j and b_j be the two terms on the right, and using (145), we obtain

$$\begin{aligned} \sum_j\Big(\sum_k p_k P_{jk}^{1/(1+\rho_3)}\Big)^{1+\rho_3} &\leq \Big[\sum_j\Big(\sum_k p_k P_{jk}^{1/(1+\rho_1)}\Big)^{1+\rho_1}\Big]^{\lambda} \\ &\quad\cdot\Big[\sum_j\Big(\sum_k p_k P_{jk}^{1/(1+\rho_2)}\Big)^{1+\rho_2}\Big]^{1-\lambda} \end{aligned} \tag{146}$$

Taking the logarithm of (146) establishes that $E_0(\rho, \mathbf{p})$ is convex upward and thus that $\partial^2 E_0/\partial\rho^2 \leq 0$. The convexity is strict unless both (144) and (145) are satisfied with equality. But condition 1) of Theorem 2 is the condition for (144) to be satisfied with equality and condition 2) is the condition for a_j and b_j to be proportional when condition 1) is satisfied.

Proof of Theorem 4: We begin by showing that $F(\rho, \mathbf{p})$ is a convex downward function of $\mathbf{p}$ for $\rho \geq 0$. From (40) we can rewrite $f(\rho, \mathbf{p})$ as

$$F(\rho, \mathbf{p}) = \sum_j \alpha_j^{1+\rho}; \qquad \alpha_j = \sum_k p_k P_{jk}^{1/(1+\rho)} \tag{147}$$

Let $\mathbf{p} = (p_1, \cdots, p_K)$ and $\mathbf{q} = (q_1, \cdots, q_K)$ be arbitrary probability vectors, and let

$$\alpha_j = \sum_k p_k P_{jk}^{1/(1+\rho)}, \quad \text{and} \quad \beta_j = \sum_k q_k P_{jk}^{1/(1+\rho)}$$

For any λ, $0 < \lambda < 1$, we have

$$\begin{aligned} &f(\rho, \lambda\mathbf{p} + (1-\lambda)\mathbf{q}) \\ &\qquad = \sum_j\Big[\sum_k (\lambda p_k + (1-\lambda)q_k)P_{jk}^{1/(1+\rho)}\Big]^{1+\rho} \\ &\qquad = \sum_j [\lambda\alpha_j + (1-\lambda)\beta_j]^{1+\rho} \end{aligned} \tag{148}$$

Since α_j and β_j must be non-negative, and since $x^{1+\rho}$ is a convex downward function of x for $\rho \geq 0$, $x \geq 0$, we can upperbound the right-hand side of (148)

$$F(\rho, \lambda\mathbf{p} + (1-\lambda)\mathbf{q}) \leq \sum_j \lambda\alpha_j^{1+\rho} + (1-\lambda)\beta_j^{1+\rho}$$

$$F(\rho, \lambda\mathbf{p} + (1-\lambda)\mathbf{q}) \leq \lambda F(\rho, \mathbf{p}) + (1-\lambda)F(\rho, \mathbf{q}) \tag{149}$$

Thus $F(\rho, \mathbf{p})$ is convex downward with $\mathbf{p}$ for $\rho \geq 0$.

The general problem of finding necessary and sufficient conditions for the vector that minimizes a differentiable convex downward function over a convex region of vector space defined by a set of inequalities has been solved by Kuhn and Tucker [17]. For the special case in which the

[10] Hardy, et al. [14], Theorem 17.

[11] The proof of convexity given here is due primarily to H. L. Yudkin.

[12] Hardy, et al., *op. cit.* [14], Theorem 17.

region is constrained by $p_k \geq 0$ for $1 \leq k \leq K$ and $\sum_k p_k = 1$, their solution reduces to

$$\frac{\partial F(\rho, \mathbf{p})}{\partial p_k} \geq u \quad \text{for all } k \text{ with equality if } p_k \neq 0 \tag{150}$$

Differentiating $F(\rho, \mathbf{p})$ and solving for the constant u, we immediately get (41). Similarly, if we substitute the convex downward function, $-I(\mathbf{p})$, in (150), then (42) follows.

Finally, we observe that $F(\rho, \mathbf{p})$ is a continuous function of $\mathbf{p}$ in the closed bounded region in which $\mathbf{p}$ is a probability vector. Therefore, $F(\rho, \mathbf{p})$ has a minimum, and thus (41) has a solution.

Proof of Theorem 7:

$$E_x(\rho, \mathbf{p}) = -\rho \ln \sum_{k,i} p_k p_i \left(\sum_j \sqrt{P_{jk}P_{ji}} \right)^{1/\rho}$$

If we make the associations $p_k p_i = q_l$, $\sum_j \sqrt{P_{jk}P_{ji}} = a_l$, and $\rho = x$, we see that the lemma applies immediately to $-E_x(\rho, \mathbf{p})$. Since $I(\mathbf{p}) \neq 0$ by assumption, $\sum_j \sqrt{P_{jk}P_{ji}}$ cannot be independent of k and i, and $E_x(\rho, \mathbf{p})$ is strictly increasing with ρ. Also, $E_x(\rho, \mathbf{p})$ is convex upward with ρ, and the convexity is strict unless $\sum_j \sqrt{P_{jk}P_{ji}}$ is always 1 or 0 for $p_k p_i \neq 0$. But $\sum_j \sqrt{P_{jk}P_{ji}} = 1$ only if $P_{jk} = P_{ji}$ for all j, and $\sum_j \sqrt{P_{jk}P_{ji}} = 0$ only if $P_{jk}P_{ji} = 0$ for all j.

References

[1] Shannon, C. E., A mathematical theory of communication, *Bell Sys. Tech. J.*, vol. 27, pp. 379, 623, 1948. See also book by same title, University of Illinois Press, Urbana, 1949.

[2] Fano, R. M., *Transmission of information*, The M.I.T. Press, Cambridge, Mass., and John Wiley & Sons, Inc., New York, N. Y., 1961.

[3] Gallager, R. G., Information theory, in *The mathematics of physics and chemistry*, H. Margenau and G. M. Murphy; Eds., D. Van Nostrand Co., Princeton, N. J., vol. 2, 1964.

[4] Wozencraft, J. M., and R. S. Kennedy, Coding and communication, presented at the URSI Conf., Tokyo, Japan, Sep 1963.

[5] Blackwell, D., and M. A. Girshick, *Theory of games and statistical decision*, John Wiley & Sons, Inc., New York, N. Y., 1954.

[6] Elias, P., Coding for two noisy channels, in *Third London Sumposium on Information Theory*, C. Cherry, Ed., Butterworth's Scientific Publications, London, England, 1955.

[7] Reiffen, B., A note on very noisy channels, *Inform. Control*, vol. 6, p. 126, 1963.

[8] Fano, R. M., private communication, 1963.

[9] Shannon, C. E., Probability of error for optimal codes in a Gaussian channel, *Bell System Tech. J.*, vol. 38, p. 611, 1959.

[10] ——, The zero-error capacity of a noisy channel, *IRE Trans. on Information Theory*, vol. IT-2, pp. 8–19, Sep 1956.

[11] Peterson, W. W., *Error correcting codes*, The M.I.T. Press, Cambridge, Mass., and John Wiley & Sons, Inc., New York, N. Y., 1961.

[12] Gallager, R. G., *Low density parity check codes*, The M.I.T. Press, Cambridge, Mass., 1963.

[13] Gnedenko, B. V., and A. N. Kolmogorov, *Limit distributions for sums of independent random variables*, Addison-Wesley Publishing Co., Cambridge, Mass., 1954.

[14] Hardy, G. H., J. E. Littlewood, and G. Polya, *Inequalities*, Cambridge University Press, Cambridge, England, Theorem 16, 1959.

[15] Kuhn, H. W., and A. W. Tucker, Nonlinear programming, in *Second Berkeley Symposium on Mathematical Statistics and Probability*, J. Neyman, Ed., University of California Press, Berkeley, p. 481, 1951.

Linear Interpolation, Extrapolation, and Prediction of Random Space-Time Fields with a Limited Domain of Measurement

D. P. PETERSEN, SENIOR MEMBER, IEEE, AND D. MIDDLETON, FELLOW, IEEE

Abstract—Formulas are derived for linear (least-square) reconstruction of multidimensional (*e.g.*, space-time) random fields from sample measurements taken over a limited region of observation. Data may or may not be contaminated with additive noise, and the sampling points may or may not be constrained to lie on a periodic lattice.

The solution of the optimum filter problem in wave-number space is possible under certain restrictive conditions: 1) that the sampling locations be periodic and occupy a *sector* of the Euclidean sampling space, and 2) that the wave-number spectrum be factorable into two components, one of which represents a function nonzero only within the data space, the other only within the sector imaging the data space through the origin.

If the values of the continuous field are accessible before sampling, a prefiltering operation can, in general, reduce the subsequent error of reconstruction. However, the determination of the optimum filter functions is exceedingly difficult, except under very special circumstances.

A one-dimensional second-order Butterworth process is used to illustrate the effects of various postulated constraints on the sampling and filtering configuration.

Introduction

IT IS OFTEN necessary, as an integral aspect of an engineering information-processing system, to derive data from measurements of random space-time fields of physical variables and to incorporate these data into decision procedures. As examples, we may cite the observation of meteorological phenomena, the scanning of radar or radio-astronomical displays, and the

Manuscript received January 29, 1964; revised July 14, 1964.

D. P. Petersen is with the Guidance and Control Dept., United Aircraft Corporate Systems Center, Farmington, Conn.

D. Middleton is with the Rensselaer Polytechnic Institute, Hartford Graduate Center, East Windsor Hill, Conn., and consulting physicist in Concord, Mass.