INFORMATION AND CONTROL 10, 522–552 (1967)

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

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

Departments of Electrical Engineering and Mathematics, Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139

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 in the January issue, summarizes the major results and treats the case of high transmission rates in detail; the second, appearing here, treats the case of low transmission rates.

1. ZERO RATE EXPONENTS

In this section we shall investigate the error probability for codes whose block length is much larger than the number of codewords, $N \gg M$. We assume throughout this section that the zero error capacity of the chan-

* The work of these authors is 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).

nel, C_0, is zero. We also assume that ordinary decoding is to be used rather than list decoding, i.e., that the list size L is one.

Our basic technique will be to bound the error probability for a given set of code words in terms of the error probability between any pair of the words, say $\underline{x}_m$ and $\underline{x}_{m'}$. We can apply the corollary to Theorem I-5, given by (I-3.20) and (I-3.21), as follows.[1] Let $P_1(\underline{y})$ and $P_2(\underline{y})$ in Theorem I-5 correspond to $\Pr(\underline{y} \mid \underline{x}_m)$ and $\Pr(\underline{y} \mid \underline{x}_{m'})$ here, and let Y_1 and Y_2 in Theorem I-5 correspond to the decoding regions Y_m and $Y_{m'}$ for the given decoding scheme here. The fact that some output sequences are decoded into messages other than m or m' in no way effects the validity of Theorem 5 or its corollary. From (I-3.20) and (I-3.21), the error probabilities $P_{e,m}$ and $P_{e,m'}$ for the given decoding scheme are bounded by either

$$P_{e,m} \geqq \tfrac{1}{4} \exp [\mu(s^*) - s^* \sqrt{2\mu''(s^*)}] \tag{1.01}$$

or

$$P_{e,m'} \geqq \tfrac{1}{4} \exp [\mu(s^*) \pm (1 - s^*) \sqrt{2\mu''(s^*)}], \tag{1.02}$$

where

$$\mu(s) = \ln \sum_{\underline{y}} \Pr(\underline{y} \mid \underline{x}_m)^{1-s} \Pr(\underline{y} \mid \underline{x}_{m'})^s \tag{1.03}$$

and s^* minimizes $\mu(s)$ over $0 \leqq s \leqq 1$.

This result can be put into a more convenient form with the aid of the following definitions.

The joint composition of $\underline{x}_m$ and $\underline{x}_{m'}$, $q_{i,k}(m, m')$ is the fraction of the positions in the block in which the ith channel input occurs in codeword $\underline{x}_m$ and the kth channel input occurs in $\underline{x}_{m'}$.

The function $\mu_{i,k}(s)$ is defined for $0 < s < 1$ by

$$\mu_{i,k}(s) \triangleq \ln \sum_j P(j \mid i)^{1-s} P(j \mid k)^s. \tag{1.04}$$

As before,

$$\mu_{i,k}(0) = \lim_{s \to 0^+} \mu_{i,k}(s)$$

and

$$\mu_{i,k}(1) = \lim_{s \to 1^-} \mu_{i,k}(s).$$

[1] References to equations, sections and theorems of the first part of this paper will be prefixed by I.

Using (I-3.10), $\mu(s)$ in (1.03) can be expressed in terms of these definitions by

$$\mu(s) = N \sum_i \sum_k q_{i,k}(m, m')\mu_{i,k}(s). \tag{1.05}$$

The *discrepancy* between $\underline{x}_m$ and $\underline{x}_{m'}$, $D(m, m')$, is defined by

$$D(m, m') \triangleq -\min_{0 \leqq s \leqq 1} \sum_i \sum_k q_{i,k}(m, m')\mu_{i,k}(s). \tag{1.06}$$

It can be seen that the quantity $\mu(s^*)$ appearing in (1.01) and (1.02) is given by $-ND(m, m')$. The discrepancy plays a role similar to that of the conventional Hamming distance for binary symmetric channels.

The *minimum discrepancy* for a code $D_{\min}$ is the minimum value of $D(m, m')$ over all pairs of code words of a particular code.

The *maximum minimum discrepancy*, $D_{\min}(N, M)$ is the maximum value of $D_{\min}$ over all codes containing M code words of block-length N.

THEOREM 1. *If $\underline{x}_m$ and $\underline{x}_{m'}$ are a pair of code words in a code of block-length N, then either*

$$P_{e,m} \geqq \frac{1}{4} \exp -N\left[D(m, m') + \sqrt{\frac{2}{N}} \ln (1/P_{\min})\right] \tag{1.07}$$

or

$$P_{e,m'} \geqq \frac{1}{4} \exp -N\left[D(m, m') + \sqrt{\frac{2}{N}} \ln (1/P_{\min})\right], \tag{1.08}$$

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

Proof. We shall show that $\mu''(s)$ is bounded by

$$\mu''(s) \leqq N\left[\ln \frac{1}{P_{\min}}\right]^2. \tag{1.09}$$

Then the theorem will follow from (1.01) and (1.02) by upper bounding s^* and $(1 - s^*)$ by 1. To establish (1.09), we use (I-3.25), obtaining

$$\mu''_{i,k}(s) = \sum_j Q_s(j)\left[\ln \frac{P(j \mid k)}{P(j \mid i)}\right]^2 - [\mu'_{i,k}(s)]^2, \tag{1.10}$$

where $Q_s(j)$ is a probability assignment over the outputs for which $P(j \mid k)$ and $P(j \mid i)$ are nonzero. Observing that

$$|\ln P(j \mid k)/P(j \mid i)| \leqq \ln (1/P_{\min}),$$

we can ignore the last term in (1.10), getting

$$\mu''_{i,k}(s) \leqq \sum_j Q_s(j)[\ln (1/P_{\min})]^2 = [\ln (1/P_{\min})]^2. \qquad (1.11)$$

Combining (1.11) with (1.05), we have (1.09), completing the proof.

Since the probability of error for the entire code of M code words is lower bounded by $P_e \geqq P_{e,m}/M$ for any m, it follows from the theorem that

$$P_e \geqq \frac{1}{4M} \exp - N\left[D_{\min} + \sqrt{\frac{2}{N}} \ln \frac{1}{P_{\min}}\right]. \qquad (1.12)$$

Conversely, we now show that there exist decoding regions such that

$$P_{e,m} \leqq (M - 1) \exp -ND_{\min} \quad \text{for all} \quad m. \qquad (1.13)$$

These regions may be chosen as follows: From Theorem I-5, there exist decoding regions $Y_m(m, m')$ and $Y_{m'}(m, m')$ for the code containing only the codewords m and m' such that both $P_{e,m}$ and $P_{e,m'}$ are no greater than $\exp -ND_{\min}$. To decode the larger code, set $Y_m = \bigcap_{m'} Y_m(m, m')$. Since the sets Y_m are not overlapping, they are legitimate decoding sets. Also, $Y_m{}^c = \bigcup_{m'} Y_m{}^c(m, m')$, and since the probability of a union of events cannot exceed the sum of their probabilities, we have

$$P_{e,m} \leqq \sum_{y \in Y_m{}^c} \Pr(y \mid x_m) \leqq \sum_{m' \neq m} \sum_{y \in Y_m{}^c(m,m')} \Pr(y \mid x_m) \qquad (1.14)$$

$$\leqq (M - 1) \exp - ND_{\min}. \qquad (1.15)$$

Combining (1.12) and (1.15) yields the first part of the following theorem:

THEOREM 2. *Let E_M be defined by*

$$\limsup_{N\to\infty} - \frac{1}{N} \ln P_e(N, M, 1).$$

Then

$$E_M = \limsup_{N\to\infty} D_{\min}(N, M) = \text{l.u.b.}_N D_{\min}(N, M) = \lim_{N\to\infty} D_{\min}(N, M). \qquad (1.16)$$

The second part of the theorem follows from the observation that we can construct a code of block length AN from a code of blocklength N by repeating every word of the original code A times. The two codes have equal $q_{i,k}(m, m')$ for all i, k, m, m', and hence they have equal $D_{\min}$.

Thus

$$D_{\min}(AN, M) \geqq D_{\min}(N, M). \tag{1.17}$$

This implies the second part of the theorem. The third part follows from (1.17) and the fact that $P_e(N, M, 1)$ is nonincreasing with N.

Theorem 2 reduces the problem of computing E_M to the problem of computing $D_{\min}(N, M)$. This computation is always easy for $M = 2$, so we treat that case first. Recall from (1.06) that $-D(m, m')$ is the minimum over s of a weighted sum of the $\mu_{i,k}(s)$. This can be lower bounded by the weighted sum of the minimums, yielding

$$-D(m, m') \geqq \sum_i \sum_k q_{i,k}(m, m') \min_{0 \leqq s \leqq 1} \mu_{i,k}(s). \tag{1.18}$$

with equality iff the same value of s simultaneously minimizes all $\mu_{i,k}(s)$ for which $q_{i,k}(m, m') > 0$. If we, set $q_{i,k}(m, m') = 1$ for the i, k pair that minimizes $\min_{0 \leqq s \leqq 1} \mu_{i,k}(s)$, then (1.18) is satisfied with equality and at the same time the right-hand side is minimized. We thus have

$$E_2 = D_{\min}(N, 2) = \max_{i,k} [- \min_{0 \leqq s \leqq 1} \mu_{i,k}(s)]. \tag{1.19}$$

It is interesting to compare this expression with the sphere packing exponent $E_{sp}(R)$ in the limit as $R \to 0$. If $R_\infty = 0$, some manipulation on (I-1.7), (I-1.8), and (I-1.9) yields

$$E_{sp}(0^+) = \lim_{\rho \to \infty} E_0(\rho) = \max_{\underline{q}} - \ln \sum_j \prod_k P(j \mid k)^{q_k} \tag{1.20}$$

Comparing (1.20) with the definition of $\mu_{i,k}(s)$ in (1.04), we see that $E_2 \leqq E_{sp}(0^+)$ with equality iff the probability vector $\underline{q}$ that maximizes (1.20) has only 2 nonzero components.

Having found the pair of input letters i, k that yield E_2, it clearly does not matter whether we set $q_{i,k}(1, 2) = 1$ or $q_{k,i}(1, 2) = 1$. However, we must *not* attempt to form some linear combination of these two optimum solutions, for by making both $q_{i,k}(1, 2)$ and $q_{k,i}(1, 2)$ nonzero we may violate the condition for equality in (1.18). For example, suppose we compare the following two codes of block length N for the completely asymmetric binary channel of Fig. I-56. The disastrous result is depicted below:

Code 1: $\underline{x}_1 = 1\ 1\ 1\ 1\ 1\ \ 1\ 1\ 1\ 1\ 1$

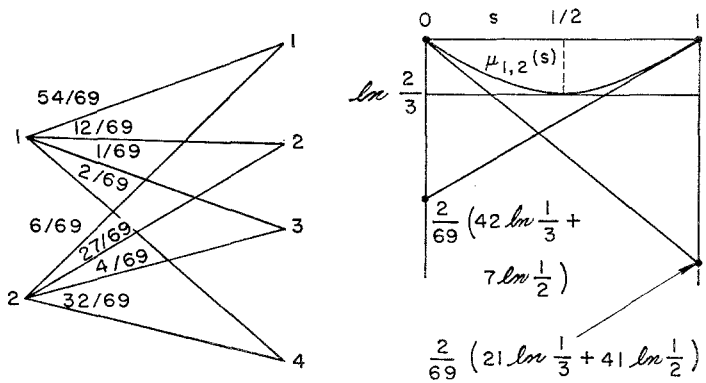


FIG. 1. A pairwise reversible binary input channel.

$$\underline{x}_2 = 2\ 2\ 2\ 2\ 2 \quad 2\ 2\ 2\ 2\ 2$$
$$\leftarrow N/2 \rightarrow \quad \leftarrow N/2 \rightarrow$$

Code 2:
$$\underline{x}_1 = 1\ 1\ 1\ 1\ 1 \quad 2\ 2\ 2\ 2\ 2$$
$$\underline{x}_2 = 2\ 2\ 2\ 2\ 2 \quad 1\ 1\ 1\ 1\ 1.$$

Using either code, an error will occur only if the received sequence consists entirely of output letter 2. For Code 1, $P_e = \frac{1}{2}p^N$; for Code 2, $P_e = \frac{1}{2}p^{N/2}$.

For a class of channels to be defined as pairwise reversible channels, this sensitivity to interchanging letters does not occur, and for these channels we shall soon see that the calculation of E_M is relatively straightforward. A channel is pairwise reversible iff, for each i, k, $\mu'_{i,k}(\frac{1}{2}) = 0$. Differentiating (1.04), this is equivalent to

$$\sum_j \sqrt{P(j \mid i)P(j \mid k)} \ln P(j \mid i) = \sum_j \sqrt{P(j \mid i)P(j \mid k)} \ln P(j \mid k); \qquad \text{all } i, k. \tag{1.21}$$

Equation (1.21) is equivalent to $\mu_{i,k}(s)$ being minimized at $s = \frac{1}{2}$ for all i, k. This guarantees that (1.18) is satisfied with equality and that a pair of inputs in the same position in a pair of code words, $\underline{x}_m$ and $\underline{x}_{m'}$, can be reversed without changing $D(m, m')$.

The class of pairwise reversible channels includes all of the symmetric binary input channels considered by Sun (1965) and Dobrushin (1962) (which are defined in a manner that guarantees that $\mu_{i,k}(s) = \mu_{k,i}(s)$

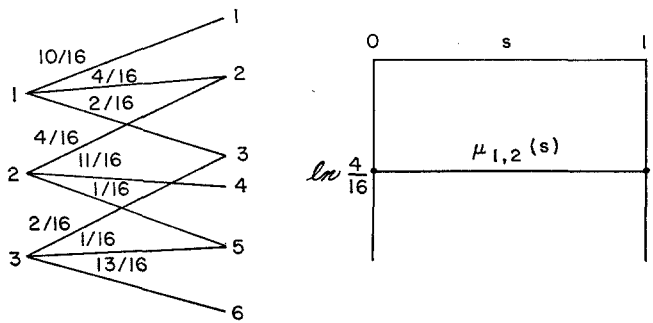


FIG. 2. A pairwise erasing ternary input channel (nonuniform but pairwise reversible).

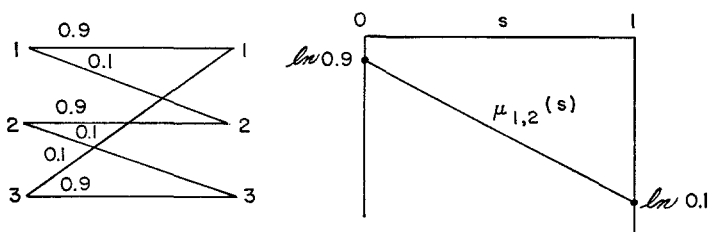


FIG. 3. A ternary unilateral channel (TUC) (uniform but not pairwise reversible).

for all s), and many other binary input channels, such as the one in Fig. 1 (as the reader is invited to verify). For multi-input channels, there is no relationship between the class of pairwise reversible channels and the uniform channels discussed by Fano (1961, p. 126). The channel of Fig. 2 is pairwise reversible but nonuniform; from any pair of inputs it looks like a binary erasure channel. The channel of Fig. 3 is not pairwise reversible even though it is uniform; from any pair of inputs it looks like an asymmetric binary erasure channel.

For pairwise reversible channels, we may compute an exact expression for E_M. To do this, we obtain a lower bound on $D_{\min}(N, M)$ which can be attained for certain values of N. The bound is derived by a method first introduced by Plotkin (1951). For any pair of code words for a pairwise reversible channel, we have[2]

[2] Readers who are familiar with the statistical literature will recognize the expression for $\mu_{i,k}(\frac{1}{2})$ as the measure of the difference between the distributions $P(j/i)$ and $P(j/k)$ which was first suggested by Helliger (1909) and later developed by Bhattacharyya (1943).

$$D(m, m') = -\sum_i \sum_k q_{i,k}(m, m')\mu_{i,k}(\tfrac{1}{2}). \tag{1.22}$$

Since the minimum discrepancy cannot exceed the average discrepancy,

$$D_{\min}(N, M) \leqq \frac{1}{M(M-1)} \sum_{m \neq m'} \sum D(m, m'). \tag{1.23}$$

The total discrepancy can be computed on a column by column basis.

$$\sum_{m=1}^{M} \sum_{m'=1}^{M} D(m, m') = -\sum_{n=1}^{N} \sum_{i=1}^{K} \sum_{k=1}^{K} M_i(n) M_k(n) \mu_{i,k}(\tfrac{1}{2}), \tag{1.24}$$

where $M_k(n)$ is the number of times the kth channel input occurs in the nth column. Let M_k^* denote the number of times the kth channel input occurs in the best possible column,

$$\max_{\Sigma M_k = M} [-\sum_i \sum_k M_i M_k \mu_{i,k}(\tfrac{1}{2})] = -\sum_i \sum_k M_i^* M_k^* \mu_{i,k}(\tfrac{1}{2}) \tag{1.25}$$

Combining (1.23) through (1.25) results in a bound for pairwise reversible channels.

$$D_{\min}(N, M) \leqq -1/(M(M-1)) \sum_i \sum_k M_i^* M_k^* \mu_{i,k}(\tfrac{1}{2}) \tag{1.26}$$

We now show that this bound can be achieved when $N = M!/\prod_k M_k^*!$ To do this, we select the first column of the code so that it has the prescribed composition, the kth channel input occurring M_k^* times. Then we choose as subsequent columns of the code all possible permutations of the first column. In the constructed code, every column contributes the same maximum amount to the total discrepancy, assuring equality between (1.24) and (1.25). Every pair of codewords is the same distance apart, assuring equality in (1.23). Because of these two facts, (1.26) holds with equality when $N = M!/(\prod_k M_k^*!)$.

This construction can likewise be used for channels that are not pairwise reversible. The constructed code has the property that $q_{i,k}(m, m') = q_{k,i}(m, m') = q_{i,k}$ independent of m and m'. This guarantees that, for this code, (1.06) is optimized by setting $s = \frac{1}{2}$, for $\mu_{i,k}(s) + \mu_{k,i}(s)$ always attains its minimum at $s = \frac{1}{2}$, even when $\mu_{i,k}(s)$ does not.

However, it may be possible to improve upon this construction for channels which are not pairwise reversible. We summarize these results in a theorem, whose proof follows directly from Theorem 2, (1.26), and the construction discussed in the preceding two paragraphs.

THEOREM 3.

$$E_M \geqq 1/(M(M-1)) \max_{\Sigma M_k = M} \sum_i \sum_k M_i M_k (-\ln \sum_j \sqrt{P(j/i)\, P(j/k)})$$

with equality for channels which are pairwise reversible.

We next compare this result with $E_{ex}(0^+)$, Gallager's (1965) lower bound to $E(0^+)$, the error exponent at infinitesimal rates. $E_{ex}(0^+)$ is given by (I-1.29) and (I-1.30) as

$$E_{ex}(0^+) = \max_{\underline{q}} \sum_i \sum_k q_i q_k (-\ln \sum_j \sqrt{P(j/i)P(j/k)}), \tag{1.27}$$

where $\underline{q}$ is the probability vector specifying the composition of the code. The vector $\underline{q}$ is unrestricted by the Diophantine constraints placed on the vector $\underline{M}^*/M$. (Here M_k^* is the kth component of $\underline{M}^*$). This additional freedom can only increase $E_{ex}(0^+)$. This proves the first of the three corollaries.

COROLLARY 3.1. *For pairwise reversible channels,*

$$E_M \leqq (M/(M-1))E_{ex}(0^+)$$

The evaluation of the expression on the right of Theorem 3 is complicated by the Diophantine constraints on the components of the vector M. To first order in M, however, these constraints may be ignored, as indicated by the following corollary.

COROLLARY 3.2. *For any channel,*

$$E_M \geqq M/(M-1)E_{ex}(0^+) - 0(1/M^2)$$

where

$$0(1/M^2) \leqq \frac{-K\mu_{\max} - \sum_{i \neq k} \sum (\mu_{i,k}(\tfrac{1}{2}) - \mu_{\max})}{4M(M-1)}.$$

Here K is the number of channel inputs and $\mu_{\max} = \max_{i \neq k} \mu_{i,k}(\frac{1}{2})$.

Since this corollary is not essential to the proof of Theorem 4, we omit its proof. The details of the straightforward but tedious calculation are given by Berlekamp (1964).

For the remainder of this section, we shall be primarily concerned with the behavior of E_M for very large M. We are especially interested in the limit of E_M as M goes to infinity, which we denote by the symbol E_∞.

Since E_M is a monotonic nonincreasing function of M, it is clear that the limit exists. As a consequence of Corollaries 3.1 and 3.2, we have

COROLLARY 3.3. $E_\infty \geqq E_{ex}(0^+)$ *with equality for channels which are pairwise reversible.*

This general inequality also follows directly from the definitions of E_∞ and $E_{ex}(0^+)$ without invoking Corollary 3.2.

We now proceed to show that Corollary 3.3 holds with equality even for channels which are not pairwise reversible.

THEOREM 4. *For any discrete memoryless channel* $E_\infty = E_{ex}(0^+)$.

Remarks. The natural approach in attempting to prove Theorem 4 would be to attempt to calculate the average discrepancy on a column by column basis as in (1.24). This direct approach does not work for channels that are not pairwise reversible, however, the difficulty being that the value of s that determines $D(m, m')$ in (1.06) is not the same as the value of s that minimizes $\mu_{i,k}(s)$ for the pairs of letters in the two code words.

We shall circumvent this difficulty by going through some manipulations on a particular subset of the code words in a code. The argument is rather lengthy and will be carried out as a sequence of 5 Lemmas. For motivation, the reader is advised to keep the ternary unilateral channel (TUC) of Figure 3 in mind throughout the proof. We begin by defining a relation of dominance between code words.

DEFINITION. $\underset{\sim}{x}_m$ dominates $\underset{\sim}{x}_{m'}$ iff

$$-\sum_i \sum_k q_{i,k}(m, m')\mu'_{i,k}(\tfrac{1}{2}) \geqq 0. \tag{1.28}$$

Notice that either $\underset{\sim}{x}_m$ dominates $\underset{\sim}{x}_{m'}$, or $\underset{\sim}{x}_{m'}$ dominates $\underset{\sim}{x}_m$, or both. This follows because

$$\mu'_{i,k}(\tfrac{1}{2}) = -\mu'_{k,i}(\tfrac{1}{2}); \qquad q_{i,k}(m, m') = q_{k,i}(m', m) \tag{1.29}$$

$$\sum_i \sum_k q_{i,k}(m', m)\mu'_{i,k}(\tfrac{1}{2}) = -\sum_i \sum_k q_{i,k}(m, m')\mu'_{i,k}(\tfrac{1}{2}). \tag{1.30}$$

For the TUC the codeword consisting of all 1's dominates any other codeword which contains at least as many 2's as 3's, but it is dominated by any other codeword which contains at least as many 3's as 2's.

Notice that dominance is *not* necessarily transitive except when the input alphabet is binary. In general, we may have $\underset{\sim}{x}$ dominate $\underset{\sim}{x}'$ and $\underset{\sim}{x}'$ dominate $\underset{\sim}{x}''$ without having $\underset{\sim}{x}$ dominate $\underset{\sim}{x}''$.

LEMMA 4.1. *If* $\underset{\sim}{x}_m$ *dominates* $\underset{\sim}{x}_{m'}$, *then*

$$D(m, m') \leqq \sum_i \sum_k q_{i,k}(m, m')[-\mu_{i,k}(\tfrac{1}{2}) - \tfrac{1}{2}\mu'_{i,k}(\tfrac{1}{2})].$$

Proof. Recall from (1.06) that

$$D(m, m') = -\min_{0 \leqq s \leqq 1} \sum_i \sum_k q_{i,k}(m, m')\mu_{i,k}(s). \tag{1.06}$$

The tangent line to a convex U function is a lower bound to the function. Taking this tangent to $\mu_{i,k}(s)$ at $s = \frac{1}{2}$ yields

$$\min_{0 \leq s \leq 1} \sum_i \sum_k q_{i,k}(m, m')\mu_{i,k}(s) \geqq \min_{0 \leq s \leq 1} \sum_i \sum_k q_{i,k}(m, m')[\mu_{i,k}(\tfrac{1}{2}) + (s - \tfrac{1}{2})\mu'_{i,k}(\tfrac{1}{2})]. \tag{1.31}$$

From the definition of dominance, (1.28), this linear function of s is minimized at $s^* = 1$.

q.e.d.

LEMMA 4.2. *From an original code containing M codewords, we may extract a subset of at least $\log_2 M$ codewords which form an "ordered" code, in which each word dominates every subsequent word.*

Proof. We first select the word in the original code which dominates the most others. According to the remarks following (1.28), this word must dominate at least half of the other words in the original code. We select this word as $\underline{x}_1$ in the ordered code. All words in the original code which are not dominated by $\underline{x}_1$ are then discarded. From the remaining words in the original code, we select the word which dominates the most others and choose it as $\underline{x}_2$ in the ordered code. The words which are not dominated by $\underline{x}_2$ are then discarded from the original code. This process is continued until all words of the original code are either placed in the ordered code or discarded. Since no more than half of the remaining words in the original code are discarded as each new word is placed in the ordered code, the ordered code contains at least $\log_2 M$ codewords.

q.e.d.

Within an ordered code, every word dominates each succeeding word. In particular, every word in the top half of the code dominates every word in the bottom half of the code. This fact enables us to bound the average discrepancy between words in the top half of the code and words in the bottom half of the code on a column by column basis. Using this technique, Lemma 4.3 gives us a bound to the minimum discrepancy of any ordered code in terms of $E_{ex}(0^+)$ and another term which must be investigated further in subsequent lemmas.

LEMMA 4.3. *Consider any ordered code having $2M$ words of block length N. The minimum discrepancy of this code is bounded by*

$$D_{\min} \leqq \sum_{m=1}^{M} \sum_{m'=M+1}^{2M} D(m, m')/M^2 \leqq E_{ex}(0^+) + 2d_{\max}\sqrt{K}\sqrt{\frac{1}{4N}\sum_{n=1}^{N}\sum_{k=1}^{K}(q_k{}^t(n) - q_k{}^b(n))^2},$$

where

$$d_{\max} \triangleq \max_{i,k} |\mu_{i,k}(\tfrac{1}{2}) + \tfrac{1}{2}\mu'_{i,k}(\tfrac{1}{2})| \tag{1.32}$$

and $\underline{q}^t(n) = [q_1{}^t(n), \cdots, q_K{}^t(n)]$ *is the composition of the* nth *column of the top half of the code* (i.e., *the* kth *channel input letter occurs* $Mq_k{}^t(n)$ *times in the* nth *column of the first* M *codewords). Similarly,* $\underline{q}^b(n) = [q_1{}^b(n), \cdots, q_K{}^b(n)]$ *is the composition of the* nth *column of the bottom half of the code.*

Proof.

$$D_{\min} \leqq \sum_{m=1}^{M} \sum_{m'=M+1}^{2M} \frac{D(m, m')}{M^2} \tag{1.33}$$

$$\leqq \sum_{m=1}^{M} \sum_{m'=M+1}^{2M} \sum_{i=1}^{K} \sum_{k=1}^{K} \frac{q_{i,k}(m, m')}{M^2} \left[- u_{i,k}(1/2) - \frac{1}{2} u'_{i,k}(1/2) \right]. \tag{1.34}$$

Now for any values of i and k,

$$\sum_{m=1}^{M} \sum_{m'=M+1}^{2M} \frac{q_{i,k}(m, m')}{M^2} = \sum_{n=1}^{N} \frac{q_i{}^t(n) q_k{}^b(n)}{N} \tag{1.35}$$

because both sides represent the average number of occurrences of the ith letter in the top half of the code opposite the kth letter in the same column of the bottom half of the code. Using this fact gives

$$D_{\min} \leqq \frac{1}{N} \sum_{n=1}^{N} \sum_{i=1}^{K} \sum_{k=1}^{K} q_i{}^t(n) q_k{}^b(n) \left[- u_{i,k}\left(\frac{1}{2}\right) - \frac{1}{2} u'_{i,k}\left(\frac{1}{2}\right) \right]. \tag{1.36}$$

This bounds $D_{\min}$ in terms of the vectors $\underline{q}^t(n)$ and $\underline{q}^b(n)$. We now introduce the vectors $\underline{q}(n)$ and $\underline{r}(n)$ defined by

$$\begin{aligned} \underline{q}(n) &\triangleq \tfrac{1}{2}[\underline{q}^t(n) + \underline{q}^b(n)] \\ \underline{r}(n) &\triangleq \tfrac{1}{2}[\underline{q}^t(n) - \underline{q}^b(n)]. \end{aligned} \tag{1.37}$$

$$\begin{aligned} \underline{q}^t(n) &= \underline{q}(n) + \underline{r}(n) \\ \underline{q}^b(n) &= \underline{q}(n) - \underline{r}(n) \end{aligned} \tag{1.38}$$

$$\begin{aligned} q_i{}^t(n) q_k{}^b(n) &= [q_i(n) + r_i(n)][q_k(n) - r_k(n)] \\ &= q_i(n) q_k(n) + r_i(n) q_k(n) - q_i{}^t(n) r_k(n). \end{aligned} \tag{1.39}$$

Since $\underline{q}(n)$ is an average of the probability vectors $\underline{q}^t(n)$ and $\underline{q}^b(n)$, $\underline{q}(n)$ is itself a probability vector. In fact, $\underline{q}(n)$ is just the composition vector for the nth column of the whole code. Since $\underline{q}(n)$ is a probability vector.

$$-\sum_i \sum_k q_i(n)q_k(n)\mu_{i,k}(\tfrac{1}{2}) \leqq \max_{\underline{q}} -\sum_i \sum_k q_i q_k \mu_{i,k}(\tfrac{1}{2}) = E_{ex}(0^+). \tag{1.40}$$

Equation (1.40) follows from (1.27) and the definition of $\mu_{i,k}$ in (1.06). Furthermore, since $\mu'_{i,k}(\tfrac{1}{2}) = -\mu'_{k,i}(\tfrac{1}{2})$, we have

$$\sum_i \sum_k q_i(n)q_k(n)\mu'_{i,k}(\tfrac{1}{2}) = 0. \tag{1.41}$$

Substituting (1.39), (1.40), and (1.41) into (1.36) gives

$$D_{\min} \leqq E_{ex}(0^+) + \frac{1}{N}\sum_{n=1}^{N}\sum_i \sum_k \left| r_i(n)q_k(n) - q_i^t(n)r_k(n) \right| \cdot \left| \mu_{i,k}\left(\frac{1}{2}\right) + \frac{1}{2}\mu'_{i,k}\left(\frac{1}{2}\right) \right| \tag{1.42}$$

$$\leqq E_{ex}(0^+) + \frac{d_{\max}}{N}\sum_{n=1}^{N}\sum_i \sum_k | r_i(n)q_k(n) - q_i^t(n)r_k(n) |, \tag{1.43}$$

where we have used the definition of $d_{\max}$ in (1.32). The remainder term is bounded as follows:

$$\begin{aligned}
&\sum_i \sum_k | r_i(n)q_k(n) - q_i^t(n)r_k(n)| \\
&\quad \leqq \sum_i \sum_k | r_i(n)q_k(n)| + | q_i^t(n)r_k(n)| \\
&\quad = \sum_k | r_k(n)| \sum_i | q_i(n)| + | q_i^t(n)| \\
&\quad = 2\sum_k | r_k(n)| \qquad (1.44) \\
&\quad \leqq 2\sqrt{K\sum_k r_k^2(n)}. \qquad (1.45)
\end{aligned}$$

Equation (1.45) follows from Cauchy's inequality which states that

$$\sum a_k b_k \leqq \sqrt{\sum_k a_k^2 \sum_k b_k^2}.$$

We have used $a_k = 1$, $b_k = | r_k(n)|$. Averaging (1.45) over all N columns gives

$$1/N \sum_{n=1}^{N}\sum_i \sum_k | r_i(n)q_k(n) - q_i^t(n)r_k(n) | \leqq \frac{2\sqrt{K}}{N}\sum_{n=1}^{N}\sqrt{\sum_{k=1}^{K} r_k^2(n)} \tag{1.46}$$

$$\leqq 2\sqrt{K}\sqrt{\frac{1}{N}\sum_{n=1}^{N}\sum_{k=1}^{K} r_k^{\,2}(n)}$$

by Cauchy. Substituting (1.37) into (1.46) completes the proof of Lemma 4.3.

Lemma 4.3 bounds the minimum discrepancy in terms of the quantity

$$\frac{1}{4N}\sum_{n=1}^{N}\sum_{k=1}^{K}(q_k^{\,t}(n) - q_k^{\,b}(n))^2 = 1/N\sum_{n,k} r_k(n)^2 = 1/N\sum_{n=1}^{N}\underline{r}(n)^2,$$

where we let $\underline{r}(n)^2$ denote the dot product of the K-dimensional vector $\underline{r}(n)$ with itself.

To complete the proof of Theorem 4, we would like to show that $1/N\sum_{n=1}^{N}\underline{r}(n)^2$ can be made arbitrarily small. Unfortunately, however, the direct approach fails, because many columns may have substantially different compositions in their top halves and their bottom halves. Nor can this difficulty be resolved by merely tightening the bound in the latter half of Lemma 4.3, for columns which are very inhomogeneous may actually make undeservedly large contributions to the total discrepancy between the two halves of the code. For example, consider a code for the *TUC* of Fig. 3. A column whose top fourth contains ones, whose middle half contains twos, and whose bottom fourth contains threes contributes $-\frac{1}{2}\ln\frac{1}{10} - \frac{1}{8}\ln\frac{9}{10}$ to the average discrepancy. We wish to show that the minimum discrepancy for this channel is actually not much better than $-\frac{1}{3}\ln\frac{1}{10} - \frac{1}{3}\ln\frac{9}{10}$. This cannot be done directly because of columns of the type just mentioned. We note, however, that this column which contributes so heavily to the average discrepancy between the top and bottom halves of the code contributes nothing to discrepancies between words in the same quarter of the block. It happens that all abnormally good columns have some fatal weakness of this sort, which we exploit by the following construction.

LEMMA 4.4. *Given an ordered code with 2M words of block length N, we can form a new code with M words of block length 2N by annexing the*

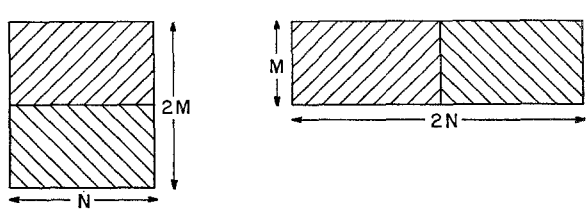


FIG. 4. Halving an ordered code.

$(M + i)$th *word to the* ith *word for all* $i = 1, \cdots, M$ *as shown in Fig.* 4. *The new code has the following properties.*

(1) *The new code is ordered.*

(2) *The minimum discrepancy of the new code is no smaller than the minimum discrepancy of the original code.*

$$\text{(3)} \quad \text{Var}(\underline{q}') - \text{Var}(\underline{q}) = \left(\frac{1}{4N}\right) \sum_{n=1}^{N} (\underline{q}'(n) - \underline{q}'(n+N))^2$$

$$\text{(4)} \quad \text{Var}(\underline{q}) \leqq \text{Var}(\underline{q}') < 1$$

where:

$\underline{q}(n)$ *is the composition of the* nth *column of the original code,* $n = 1, 2, \cdots, N$.

$\underline{q}'(n)$ *is the composition of the* nth *column of the new code,* $n = 1, 2, \cdots, 2N$.

$$\bar{\underline{q}} = 1/N \sum_{n=1}^{N} \underline{q}(n)$$

$$\bar{\underline{q}}' = 1/2N \sum_{n=1}^{2N} \underline{q}'(n)$$

$$\text{Var}(\underline{q}) = 1/N \sum_{n=1}^{N} (\underline{q}(n) - \bar{\underline{q}})^2 = \left[\frac{1}{N} \sum_{n=1}^{N} \underline{q}(n)^2\right] - \bar{\underline{q}}^2$$

$$\text{Var}(\underline{q}') = 1/2N \sum_{n=1}^{2N} (\underline{q}'(n) - \bar{\underline{q}}')^2 = \left[\frac{1}{2N} \sum_{n=1}^{2N} \underline{q}'(n)^2\right] - \bar{\underline{q}}'^2.$$

Proof of Property 1. Let $q'_{i,k}(m, m')$ be the joint composition of the mth and m'th words in the new code, i.e., the fraction of times that the ith channel input letter occurs in the mth word of the new code opposite the kth channel input letter in the m'th word. By the halving construction which generated the new code (Fig. 4),

$$q'_{i,k}(m, m') = \tfrac{1}{2}[q_{i,k}(m, m') + q_{i,k}(m + M, m' + M)]. \quad (1.47)$$

If $m < m'$, then, in the original code

$$-\sum_i \sum_k q_{i,k}(m, m')\mu'_{i,k}(\tfrac{1}{2}) \geqq 0$$

$$-\sum_i \sum_k q_{i,k}(m + M, m' + M)\mu'_{i,k}(\tfrac{1}{2}) \geqq 0$$

Consequently, in the new code

$$-\sum_i \sum_k q'_{i,k}(m, m')\mu'_{i,k}(\tfrac{1}{2}) \geqq 0. \quad (1.48)$$

Proof of Property 2. In the new code,

$$D'(m, m') = \tfrac{1}{2}[D(m, m') + D(m + M, m' + M)].$$

Thus $D'(m, m')$ can not be smaller than both $D(m, m')$ and $D(m + M, m' + M)$.

Proof of Property 3. $\underline{q}(n) = \tfrac{1}{2}[\underline{q}'(n) + \underline{q}'(n + N)]$

$$\bar{\underline{q}} = \frac{1}{2N} \sum_{n=1}^{N} [\underline{q}'(n) + \underline{q}'(n + N)] = \bar{\underline{q}}' \tag{1.49}$$

$$\begin{aligned} \text{Var } (\underline{q}') - \text{Var } (\underline{q}) &= \left(\frac{1}{2N} \sum_{n=1}^{2N} \underline{q}'(n)^2\right) - \left(\frac{1}{N} \sum_{n=1}^{N} \underline{q}(n)^2\right) \\ &= \frac{1}{4N} \sum_{n=1}^{N} \{2[\underline{q}'(n)^2 + \underline{q}'(n + N)^2] - (\underline{q}'(n) \\ &\qquad + \underline{q}'(n + N))^2\} \qquad (1.50) \\ &= \frac{1}{4N} \sum_{n=1}^{N} (\underline{q}'(n) - \underline{q}'(n + N))^2. \end{aligned}$$

Proof of Property 4. From Property 3, Var $(\underline{q}) \leqq$ Var $(\underline{q}')$. Also, for every n,

$$[\underline{q}'(n)]^2 = \sum_k [q_k'(n)]^2 \leqq 1 \tag{1.51}$$

$$\text{Var } (\underline{q}') \leqq \frac{1}{2N} \sum_{n=1}^{2N} [\underline{q}'(n)]^2 \leqq 1. \tag{1.52}$$

We may now complete the proof of the theorem by iterating the halving construction to prove Lemma 4.5.

LEMMA 4.5.

$$D_{\min}(N, M) < E_{ex}(0^+) + \frac{2d_{\max}\sqrt{K}}{\sqrt{[\log (\log M)]^-}} \tag{1.53}$$

Proof. Starting from any original code containing M codewords of block length N, we may extract a subset of $2^{[\log(\log M)]^-}$ code words which form an ordered code. This follows from Lemma 4.2 and the observation that $2^{[\log(\log M)]^-} \leqq \log M$. (Here $[\log (\log M)]^-$ is the largest integer less than or equal to $\log (\log M)$.)

We next halve the ordered code $[\log (\log M)]^-$ times. This gives us a sequence of $[\log (\log M)]^- + 1$ codes, starting with the original ordered code and terminating with a degenerate code containing only one codeword of block length $N2^{[\log(\log M)]^-}$. Since the properties of Lemma 4.4

are hereditary, every code in the sequence is ordered and each code has a minimum discrepancy no smaller than any of its ancestors (except the final degenerate code, for which the minimum discrepancy is undefined). The average variance of the column compositions of each of these codes is at least as great as the average variance of the column compositions of the preceding codes; yet the average variance of each code in the sequence must be between zero and one. Consequently, this sequence of $[\log (\log M)]^{-} + 1$ codes must contain two consecutive codes for which the difference in the variance of column compositions is less than $1/[\log (\log M)]^{-}$. The former of these two consecutive codes is non-degenerate, and Lemma 4.3 applies, with

$$\begin{aligned}\frac{1}{4N}\sum_{n=1}^{N}\sum_{k=1}^{K}(q_k{}^{t}(n) - q_k{}^{b}(n))^2 &= \frac{1}{4N}\sum_{n=1}^{N}(\underline{q}'(n) - \underline{q}'(n+N))^2 \\ &= \mathrm{Var}\,(\underline{q}') - \mathrm{Var}\,(\underline{q}) < 1/[\log (\log M)]^{-}\end{aligned} \tag{1.54}$$

q.e.d.

Theorem 4 follows directly from Lemma 4.5 and Theorem 2.

q.e.d.

Combining (1.53) and (1.12), we obtain an explicit bound on $P_e(N, M, 1)$.

$$P_e(N, M, 1) \geqq \exp - N\left[E_{ex}(0^{+}) + \frac{2d_{\max}\sqrt{K}}{\sqrt{[\log (\log M)]^{-}}} + \sqrt{\frac{2}{N}}\ln\frac{1}{P_{\min}} + \frac{\ln 4M}{N}\right] \tag{1.55}$$

If we upper bound $d_{\max}$, as given by (1.32) by

$$d_{\max} \leqq 2\max_{i,k}|\mu_{i,k}(\tfrac{1}{2})|,$$

then (1.55) becomes equivalent to (I-1.17) and we have completed the proof of Theorem I-3.

Equation (1.55) has a rather peculiar behavior with M. On the other hand, $P_e(N, M, 1)$ must be a monotone nondecreasing function of M, and thus for any M greater than some given value, we can use (1.55) evaluated at that given M. It is convenient to choose this given M as $2^{\sqrt{N}-}$, yielding

$$P_e(N, M, 1) \geqq \exp - N[E_{ex}(0^{+}) + o_4(N)]; \qquad M \geqq 2^{\sqrt{N}} \tag{1.56}$$

where

$$o_4(N) = \frac{2d_{\max}\sqrt{K}}{\sqrt{[\log N]^-}} + \sqrt{\frac{2}{N}} \ln \frac{1}{P_{\min}} + \frac{\ln 2}{\sqrt{N}} + \frac{2 \ln 2}{N}. \quad (1.57)$$

These equations can now be restated in a form similar to our other bounds on $P_e(N, M, 1)$.

THEOREM 5.

$$P_e(N, M, 1) \geqq \exp -N[E_{lr}(R - o_3(N)) + o_4(N)], \quad (1.58)$$

where

$$E_{lr}(R) = \begin{cases} E_{ex}(0^+); & R \geqq 0 \\ \infty; & R < 0 \end{cases} \quad (1.59)$$

$$o_3(N) = \frac{\ln 2}{\sqrt{N}}. \quad (1.60)$$

Proof. Observe that when $M \geqq 2^{\sqrt{N}}$ we have $R = (\ln M)/N \geqq (\ln 2)/\sqrt{N}$ and (1.58) reduces to (1.56). For $M < 2^{\sqrt{N}}$, (1.58) simply states that $P_e(N, M, 1) \geqq 0$.

2. THE STRAIGHT LINE BOUND

We have seen that the sphere packing bound (Theorem I-2) specifies the reliability of a channel at rates above R_{crit} and that the zero rate bound (Theorem I-3 or Theorem 5) specifies the reliability in the limit as the rate approaches zero. In this section, we shall couple these results with Theorem I-1 to establish the straight line bound on reliability given in Theorem I-4. Actually we shall prove a somewhat stronger theorem here which allows us to upper bound the reliability of a channel by a straight line between the sphere packing exponent and any low rate, exponential bound on error probability.

THEOREM 6. *Let $E_{lr}(R)$ be a nonincreasing function of R (not necessarily that given by (1.59)), let $o_3(N)$ and $o_4(N)$ be nonincreasing with N and let $No_3(N)$ and $No_4(N)$ be nondecreasing with N. Let $R_2 < R_1$ be nonnegative numbers and define the linear function*

$$E_{sl}(R_0) = \lambda E_{sp}(R_1) + (1 - \lambda)E_{lr}(R_2), \quad (2.01)$$

where E_{sp} is given by (I-1.07) and λ is given by

$$R_0 = \lambda R_1 + (1 - \lambda)R_2. \quad (2.02)$$

If

$$P_e(N, M, 1) \leqq \exp - N[E_{lr}(R - o_3(N)) + o_4(N)] \quad (2.03)$$

is valid for arbitrary positive M, N, *then*

$$P_e(N, M, 1) \leqq \exp - N\{E_{sl}[R - o_5(N)] + o_6(N)\} \quad (2.04)$$

is valid for

$$R_2 \leqq R - o_5(N) \leqq R_1 , \quad (2.05)$$

where

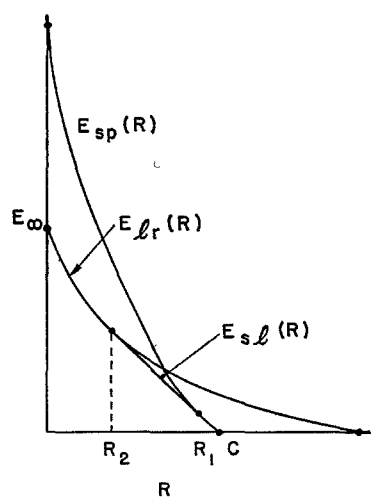
$$o_5(N) = o_1(N) + o_3(N) + R_2/N \quad (2.06)$$

$$o_6(N) = o_2(N) + o_4(N) + \frac{1}{N} E_{lr}(R_2) \quad (2.07)$$

and $o_1(N)$ *and* $o_2(N)$ *are given by* (I-1.10) *and* $R = (\ln M)/N$.

Remarks. As shown in Figs. 5–8, $E_{sl}(R)$ is a straight line joining $E_{lr}(R_2)$ at R_2 to $E_{sp}(R_1)$ at R_1. It is clearly desirable, in achieving the best bound, to choose R_1 and R_2 so as to minimize $E_{sl}(R)$. If $E_{lr}(R)$ is not convex $\cup$, it may happen, as in Fig. 8 that the best choice of R_1, R_2 depends on R.

Theorem I-4 of the introduction is an immediate consequence of Theorem 6, obtained by choosing $E_{lr}(R)$ as in Theorem 5 and choosing



FIGS. 5–8. Geometric construction for $E_{sl}(R)$.

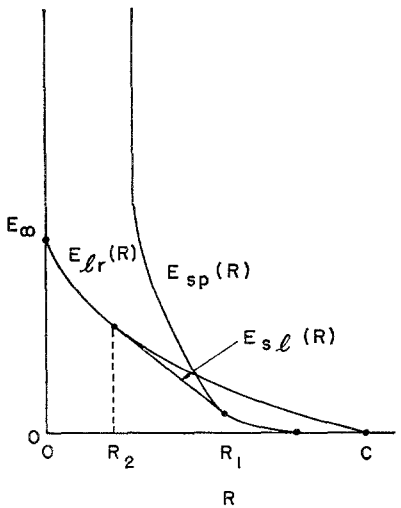


FIG. 6

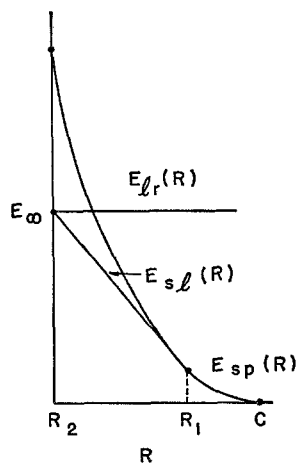


FIG. 7

$R_2 = 0$. The increased generality of Theorem 6 over Theorem I-4 is non-empty, however. In Theorem 8 we shall give an example of a low rate bound for the binary symmetric channel in which $E_{lr}(R)$ behaves as in Fig. 5.

The restriction in the theorem that $E_{lr}(R)$ be nonincreasing with R is no real restriction. Since $P_e(N, M, 1)$ is nonincreasing with M, any

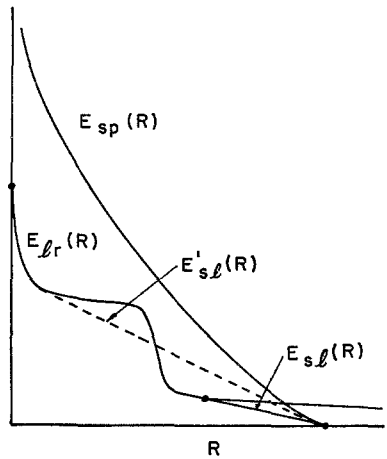


FIG. 8

bound in which $E_{lr}(R)$ is increasing with R can be tightened to a bound in which $E_{lr}(R)$ is not increasing. Likewise the restriction that $No_3(N)$ and $No_4(N)$ be increasing with N is not serious since any bound can be weakened slightly to satisfy this restriction.

Proof. By Theorem I-1, we have

$$P_e(N, M, 1) \geqq P_e(N_1, M, L)P_e(N_2, L + 1, 1), \tag{2.08}$$

where $N_1 + N_2 = N$ and L is an arbitrary positive integer. Applying the sphere packing bound, Theorem I-2, to $P_e(N_1, M, L)$ and applying (2.03) to $P_e(N_2, L + 1, 1)$, we have

$$\begin{aligned} P_e(N, M, 1) \geqq \exp\Bigg\{ &-N_1\left[E_{sp}\left(\frac{\ln M/L}{N_1} - o_1(N_1)\right) + o_2(N_1)\right] \\ &- N_2\left[E_{lr}\left(\frac{\ln (L+1)}{N_2} - o_3(N_2)\right) + o_4(N_2)\right]\Bigg\}. \end{aligned} \tag{2.09}$$

Using the expressions for $o_1(N)$ and $o_2(N)$ in (I-1.10), we see that $No_i(N)$ is increasing with N for $i = 1, 2, 3, 4$. Thus we can lower bound (2.09) by

$$\begin{aligned} P_e(N, M, 1) \geqq \exp\Bigg\{ &-N_1E_{sp}\left(\frac{\ln M/L}{N_1} - \frac{No_1(N)}{N_1}\right) - No_2(N) \\ &- N_2E_{lr}\left(\frac{\ln (L+1)}{N_2} - \frac{No_3(N)}{N_2}\right) - No_4(N)\Bigg\} \end{aligned} \tag{2.10}$$

This is valid for any positive integers N_1 and N_2 summing to N, and we observe that it is trivially valid if either N_1 or N_2 is 0.

We next get rid of the restrictions that L, N_1, and N_2 be integers. Let $\tilde{L}$ be an arbitrary real number between L and $L + 1$. We can lower bound the right-hand side of (2.10) by replacing $\ln M/L$ with $\ln M/\tilde{L}$ and $\ln (L + 1)$ with $\ln \tilde{L}$. Similarly, let $\tilde{N}_1$ be an arbitrary real number between N_1 and $N_1 + 1$. The right-hand side of (2.10) can be lower bounded by replacing N_1 with $\tilde{N}_1$. Finally, since $N_2 \leqq N - \tilde{N}_1 + 1$, we can lower bound (2.10) by replacing N_2 with $N - \tilde{N}_1 + 1$. Making these changes, we have

$$P_e(N, M, 1) \geqq \exp\left\{-\tilde{N}_1 E_{sp}\left(\frac{\ln (M/\tilde{L}) - No_1(N)}{\tilde{N}_1}\right)\right.$$
$$\left. - N[o_2(N) + o_4(N)] - (N - \tilde{N}_1 + 1)E_{lr}\left(\frac{\ln \tilde{L} - No_3(N)}{N - \tilde{N}_1 + 1}\right)\right\} \tag{2.11}$$

Define λ to satisfy

$$R - o_5(N) = \lambda R_1 + (1 - \lambda)R_2 \tag{2.12}$$

From the restriction (2.05), λ satisfies $0 \leqq \lambda \leqq 1$. Now choose $\tilde{N}_1$ and $\tilde{L}$ by

$$\tilde{N}_1 = \lambda N \tag{2.13}$$

$$\ln \tilde{L} = R_2(N - \tilde{N}_1 + 1) + No_3(N). \tag{2.14}$$

By rearranging (2.14), we see that the argument of E_{lr} in (2.11) satisfies

$$\frac{\ln \tilde{L} - No_3(N)}{N - \tilde{N}_1 + 1} = R_2 \tag{2.15}$$

Likewise, using (2.12), (2.13), (2.14), and (2.06), the argument of E_{sp} in (2.11) is given by

$$\frac{\ln(M/\tilde{L}) - No_1(N)}{\tilde{N}_1} = \frac{1}{\lambda}\left[\frac{\ln M}{N} - \frac{\ln \tilde{L}}{N} - o_1(N)\right]$$
$$= \frac{1}{\lambda}\left[R - R_2\left(1 - \lambda + \frac{1}{N}\right) - o_1(N) - o_2(N)\right]$$
$$= \frac{1}{\lambda}[R - R_2(1 - \lambda) - o_5(N)] = R_1. \tag{2.16}$$

Substituting (2.15) and (2.16) into (2.11), we have

$$P_e(N, M, 1) \geqq \exp - N\left\{\lambda E_{sp}(R_1) + \left(1 - \lambda + \frac{1}{N}\right) E_{lr}(R_2) + o_2(N) + o_4(N)\right\} \tag{2.17}$$

Combining (2.12), (2.02), and (2.01), we have

$$E_{sl}(R - o_5(N)) = \lambda E_{sp}(R_1) + (1 - \lambda) E_{lr}(R_2) \tag{2.18}$$

Finally, substituting (2.18) and (2.07) into (2.17), we have (2.04), completing the proof.

The straight line bound $E_{sl}(R)$ depends critically on the low rate bound $E_{lr}(R)$ to which it is joined. If the low rate bound is chosen as E_∞, then the resulting straight line bound $E_{sl}(R)$ is given by Theorem I-4. Plots of this bound for several channels are shown in Figure I-4.

From the discussion following (1.20), we see that if $C \neq 0$ and $C_0 = 0$, then E_∞ is strictly less than $E_{sp}(0^+)$, and the straight line bound $E_{sl}(R)$ of Theorem 4 exists over a nonzero range of rates. Also it follows from Theorem 7 of Gallager (1965) that $E_{ex}(R)$ is strictly convex $\cup$ and therefore is strictly less than $E_{sl}(R)$ in the interior of this range of rates.

There is an interesting limiting situation, however, in which $E_{sl}(R)$ and $E_{ex}(R)$ virtually coincide. These are the very noisy channels, first introduced by Reiffen (1963) and extended by Gallager (1965). A very noisy channel is a channel whose transition probabilities may be expressed by

$$P(j \mid k) = r_j(1 + \epsilon_{j,k}), \tag{2.19}$$

where r_j is an appropriate probability distribution defined on the channel outputs and $|\epsilon_{j,k}| \ll 1$ for all j and k. The function $E_0(\rho)$ for such a channel can be expanded as a power series in $\epsilon_{j,k}$. By neglecting all terms of higher than second order, Gallager (1965) obtained

$$E_0(\rho) = \frac{\rho}{1 + \rho} C, \tag{2.20}$$

where the capacity C is given by

$$C = \max_{\underline{q}} \tfrac{1}{2} \sum_j r_j[\sum_k q_k \epsilon_{j,k}^2 - (\sum_k q_k \epsilon_{j,k})^2] \tag{2.21}$$

$$= \max_{\underline{q}} \tfrac{1}{4} \sum_i \sum_k q_i q_k \sum_j r_j(\epsilon_{j,i}^2 + \epsilon_{j,k}^2 - 2\epsilon_{j,i}\epsilon_{j,k}). \tag{2.22}$$

The resulting random coding exponent is given by

$$E_r(R) = (\sqrt{C} - \sqrt{R})^2 \quad \text{for} \quad C/4 \leqq R \leqq C \tag{2.23}$$

$$= C/2 - R \qquad \text{for} \quad R < C/4. \tag{2.24}$$

We can calculate E_∞ in the same way

$$E_\infty = \max_{\underline{q}} -\sum_i \sum_k q_i q_k \ln \sum_j \sqrt{P(j \mid i)P(j \mid k)}. \tag{I-1.18}$$

Using (2.19) and expanding to second order in ϵ, gives

$$\sum_j \sqrt{P(j \mid i)P(j \mid k)} = \sum_j r_j(1 + \epsilon_{j,i}/2 - \epsilon_{j,i}^2/8) \cdot (1 + \epsilon_{j,k}/2 - \epsilon_{j,k}^2/8). \tag{2.25}$$

From (2.19) we observe that

$$\sum_j r_j \epsilon_{j,k} = 0 \quad \text{for all} \quad k \tag{2.26}$$

$$\sum_j \sqrt{P(j \mid i)P(j \mid k)} = 1 - \tfrac{1}{8} \sum_j r_j(\epsilon_{j,i}^2 + \epsilon_{j,k}^2 - 2\epsilon_{j,i}\,\epsilon_{j,k}). \tag{2.27}$$

From (2.27), (I-1.18), and (2.22), we conclude that

$$E_\infty = C/2 = E_r(0). \tag{2.28}$$

Thus in the limit as the $\epsilon_{j,k}$ approach 0, the upper and lower bounds to the reliability $E(R)$ come together at all rates and (2.23) and (2.24) give the reliability function of a very noisy channel.

For channels which are not very noisy, the actual reliability may lie well below the straight line bound from E_∞ to the sphere packing bound. As a specific case in which these bounds may be improved, we consider the binary symmetric channel.

This channel has received a great deal of attention in the literature, primarily because it provides the simplest context within which most coding problems can be considered. The minimum distance of a code, $d_{\min}$, is defined as the least number of positions in which any two code words differ. We further define $d(N, M)$ as the maximum value of $d_{\min}$ over all codes with M code words of length N. Here we are interested primarily in the asymptotic behavior of $d(N, M)$ for large N and M and fixed $R = (\ln M)/N$. The *asymptotic distance ratio* is defined as

$$\delta(R) \triangleq \limsup_{N \to \infty} \frac{1}{N} d(N, [e^{RN}]^+). \tag{2.29}$$

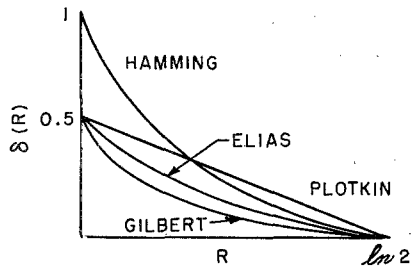


FIG. 9. Comparison of bounds on minimum distance for a binary symmetric channel.

There are two well known upper bounds to $\delta(R)$, due to Hamming (1950) and Plotkin (1951), and one well known lower bound due to Gilbert (1952). These are given implicitly by

$$\ln 2 - H(\delta(R)/2) \geqq R \qquad \text{(Hamming)} \tag{2.30}$$

$$\ln 2 - 2\delta(R) \ln 2 \geqq R \qquad \text{(Plotkin)} \tag{2.31}$$

$$\ln 2 - H(\delta(R)) \leqq R \qquad \text{(Gilbert)}, \tag{2.32}$$

where

$$H(\delta) = -\delta \ln \delta - (1 - \delta) \ln (1 - \delta). \tag{2.33}$$

See Peterson (1961) for an excellent discussion of these bounds.

Here we shall derive a third upper bound to $\delta(R)$, derived by Elias in 1960 but as yet unpublished. As shown in Fig. 9 the Elias bound is stronger than either the Hamming or Plotkin bounds for $0 < R < \ln 2$. It should be observed, however, that this superiority applies only to the asymptotic quantity, $\delta(R)$. For sufficiently small values of N, M there are a number of bounds on $d(N, M)$ which are stronger than the Elias bound.

THEOREM 7 (Elias).

$$\delta(R) \leqq 2\lambda_R(1 - \lambda_R), \tag{2.34}$$

where λ_R *is given by*

$$\ln 2 - H(\lambda_R) = R; \qquad 0 \leqq \lambda_R \leqq \tfrac{1}{2}. \tag{2.35}$$

Before proving this theorem, we shall discuss the relationship between $\delta(R)$ and the reliability function $E(R)$. Suppose that a code contains two code words at a distance d apart. From I-3.10, $\mu(s)$ for these two

words is given by $d \ln [p^s q^{1-s} + q^s p^{1-s}]$, where p is the cross-over probability of the channel (see Fig. I-5a) and $q = 1 - p$. This is minimized at $s = \frac{1}{2}$, and from (I-3.20) and (I-3.21), one of the code words has an error probability bounded by

$$P_{e,m} \geqq \frac{1}{4} \exp \left[d \ln 2\sqrt{pq} - \sqrt{\frac{d}{2}} \ln \frac{1}{p} \right], \tag{2.36}$$

where we have used (1.11) in bounding $\mu''(\frac{1}{2})$.

Next, for a code with $2M$ code words of block length N, we see by expurgating M of the worst words that at least M code words have a distance at most $d(N, M)$ from some other code word. For such a code

$$P_e \geqq \frac{1}{8} \exp \left[-d(N, M) \ln 2 \sqrt{pq} - \sqrt{d(N, M)/2} \ln \frac{1}{p} \right]. \tag{2.37}$$

Combining (2.37) with (2.29), we obtain

$$P_e(N, M, 1) \geqq \exp -N[\delta(R) \ln 2 \sqrt{pq} + o(N)] \tag{2.38}$$

$$E(R) \leqq \frac{\delta(R)}{2} \ln 4pq. \tag{2.39}$$

Conversely, if a code of block length N has minimum distance $\delta(R)N$, then it is always possible to decode correctly when fewer than $\frac{1}{2}\delta(R)N$ errors occur. By using the Chernov (1952) bound, if $p < \frac{1}{2}\delta(R)$, the probability of $\frac{1}{2}\delta(R)N$ or more errors is bounded by

$$P_e \leqq \exp - N \left[-\frac{\delta(R)}{2} \ln p - \left(1 - \frac{\delta(R)}{2}\right) \ln q - H\left(\frac{\delta(R)}{2}\right) \right] \tag{2.40}$$

$$E(R) \geqq -\frac{\delta(R)}{2} \ln p - \left(1 - \frac{\delta(R)}{2}\right) \ln q - H\left(\frac{\delta(R)}{2}\right). \tag{2.41}$$

For more complete discussions of techniques for bounding the error probability on a binary symmetric channel, see Fano (1961), Chap. 7 or Gallager (1963), Chap. 3. The bounds on reliability given by (2.39) and (2.41) are quite different, primarily because it is usually possible to decode correctly when many more than $\frac{1}{2}\delta(R)N$ errors occur. As p becomes very small, however, the minimum distance of the code becomes increasingly important, and dividing (2.39) and (2.41) by $-\ln p$, we see that

$$\frac{\delta(R)}{2} = \lim_{p \to 0} \frac{E(R)}{-\ln p}. \tag{2.42}$$

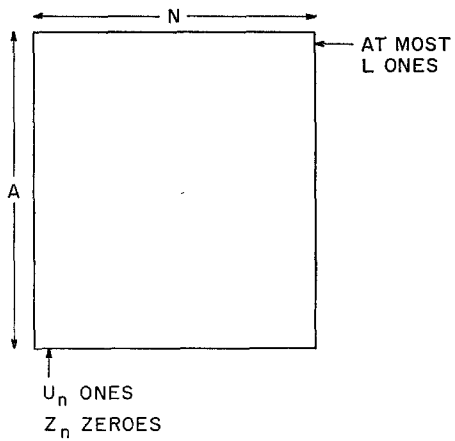


FIG. 10. Construction for Elias bound.

Along with (2.42), there are several other interesting connections between $E(R)$ and $\delta(R)$. For example, if one could show that $\delta(R)$ was given by the Gilbert bound (2.32) with equality, then upon substituting (2.32) into (2.39) one would find an *upper* bound for reliability which is equal to the lower bound $E_{ex}(R)$ over the range of rates for which $E_{ex}(R) > E_r(R)$. By combining this with Theorem 6, $E(R)$ would be determined for all rates and would be equal to the known lower bound to $E(R)$. Thus the question of determining $E(R)$ for the *BSC* hinges around the problem of determining $\delta(R)$.

Proof of Theorem 7. The proof of the Elias bound combines the arguments of Plotkin and Hamming in an ingenious way. For any integer L, $0 \leqq L \leqq N/2$, there are $\sum_{i=0}^{L} \binom{N}{i}$ binary N-tuples within a sphere of radius L around any given code word (i.e., N-tuples that have a distance L or less from the code word). For M code words, these spheres contain $M \sum_{i=0}^{L} \binom{N}{i}$ N-tuples, counting an N-tuple once for each appearance in a sphere. Since there are only 2^N different binary N-tuples, some critical N-tuple must appear in at least A spheres where

$$A \triangleq \left[2^{-N} M \sum_{i=0}^{L} \binom{N}{i} \right]^{+}. \tag{2.43}$$

Thus this critical N-tuple contains at least A code words within a sphere of radius L around itself.

For the remainder of the proof, we consider only these A code words and we assume that L is chosen so that $A \geqq 2$. For convenience we translate these code words by subtracting the critical word from each of them. Each of the A translated code words then has at most L ones.

We next list the A translated code words as in Fig. 10. Let U_n denote the number of ones in the nth column Z_n, the number of zeroes. The total number of ones in the $A \times N$ matrix of Fig. 10 may be computed either by summing along the columns or along the rows. This gives

$$\sum_n U_n \leqq AL. \tag{2.44}$$

We now compute the total distance among the $\binom{A}{2}$ pairs of translated code words. The contribution to the total distance from the nth column is $U_n Z_n$. Consequently,

$$d_{\text{tot}} = \sum_n U_n Z_n. \tag{2.45}$$

Since the minimum distance cannot exceed the average distance, we have

$$d_{\min} \leqq d_{\text{tot}} \Big/ \binom{A}{2} = \sum_{n=1}^{N} U_n(A - U_n) \Big/ \binom{A}{2}. \tag{2.46}$$

The function $\sum_{n=1}^{N} U_n(A - U_n)$ is a concave function of the U_n, and is therefore maximized, subject to the constraint (2.44), by making the partial derivation with respect to U_n a constant. Thus the maximum occurs with $U_n = AL/N$ for all n:

$$d_{\min} \leqq \frac{2NA^2\left(\frac{L}{N}\right)\left(1 - \frac{L}{N}\right)}{A(A-1)} = 2N(L/N)(1 - L/N)\left(1 + \frac{1}{A-1}\right) \tag{2.47}$$

$$\frac{d_{\min}}{N} \leqq 2(L/N)(1 - L/N) + \frac{1}{2(A-1)}. \tag{2.48}$$

Since (2.48) is valid for any L such that $A \geqq 2$, L can be chosen so as to optimize the bound. In the theorem, however, we are interested in asymptotic results for fixed R, large N, and $M = [e^{NR}]^+$. First we lower bound A.

Shannon[3] has shown that

$$\binom{N}{L} \geqq [8L(N-L)/N]^{-1/2} \exp NH(L/N). \tag{2.49}$$

The first term is lower bounded by taking $L = N/2$, yielding

$$\sum_{i=0}^{L} \binom{N}{i} > \binom{N}{L} \geqq \frac{1}{\sqrt{2N}} \exp NH(L/N). \tag{2.50}$$

Next, choose L to satisfy

$$H\left(\frac{L-1}{N}\right) < \ln 2 - \frac{\ln M}{N} + \frac{3}{2}\frac{\ln N}{N} \leqq H\left(\frac{L}{N}\right). \tag{2.51}$$

Observe that for any fixed $R > 0$, this will have a solution for large enough N. Combining (2.43), (2.50), and (2.51) we obtain

$$A > \sqrt{\frac{1}{2N}} \exp\left[\frac{3}{2}\ln N\right] = \frac{N}{\sqrt{2}} \tag{2.52}$$

Next recalling the definition of λ_R in (2.35), the left-hand side of (2.51) becomes

$$H\left(\frac{L-1}{N}\right) < H(\lambda_R) + \frac{3}{2}\frac{\ln N}{N}. \tag{2.53}$$

Since H is a concave $\cap$ function, we can combine (2.53) with the result that $H(\frac{1}{2}) = \ln 2$ to obtain

$$\frac{L-1}{N} < \lambda_R + \left(\frac{3}{2}\frac{\ln N}{N}\right)\left[\frac{\ln 2 - H(\lambda_R)}{\frac{1}{2} - \lambda_R}\right] \tag{2.54}$$

Substituting (2.52) and (2.54) into (2.48), we have

$$\frac{d(N,M)}{N} \leqq 2\lambda_R(1-\lambda_R) + o(N), \tag{2.55}$$

where $o(N)$ can be taken as

$$o(N) = 3\frac{\ln N}{N}\left(\frac{\ln 2 - H(\lambda_R)}{\frac{1}{2} - \lambda_R}\right) + \frac{2}{N} + \frac{1}{\sqrt{2N-2}}. \tag{2.56}$$

If we now substitute the Elias bound (2.34) into (2.39), we get a new upper bound on reliability given by:

THEOREM 8. *For a binary symmetric channel, an upper bound on relia-*

[3] C. E. Shannon, unpublished seminar notes, M. I. T., 1956. For a published derivation, see Ash (1965), p. 113.

bility is given by

$$E(R) \leqq E_{lr}(R) = -\lambda_R(1 - \lambda_R) \ln 4pq, \qquad (2.57)$$

where λ_R *is given by* (2.35).

RECEIVED: January 18, 1966

REFERENCES

ASH, R. B. (1965), "Information Theory." Wiley (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**(3), 99–110.

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

DOBRUSHIN, (1962), "Optimal binary codes for small rates of transmission of information," *Theory of Probability and its Applications*, Vol. 7, p. 199–204.

ELIAS, P. (1955), List decoding for noisy channels. *Tech. Report 335.* Research Laboratory of Electronics, M.I.T., Cambridge.

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

FEINSTEIN, A. (1955), Error bounds in noisy channels without memory. *IEEE Trans.* **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, Cambridge.

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

GALLAGER, R. (1965), Lower bounds on the tails of probability distributions. M.I.T. Research Laboratory of Electronics, OPR 77, 277–291.

GILBERT, E. N. (1952), A comparison of signalling alphabets. *BSTJ* **3,** 504–522.

HAMMING, R. W. (1950), Error detecting and error correcting codes. *BSTJ* **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.* **IT-13** (to appear).

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, Cambridge, and Wiley, New York.

PLOTKIN, M. (1960), Research Division Report 51-20, University of Pennsylvania. Eventually published in 1960 as: Binary codes with specified minimum distance. *PGIT* **IT6,** 445–450.

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

SHANNON, C. E. (1948), A mathematical theory of communication. *BSTJ* **27**, 379, 623. Also in book form with postscript by W. Weaver, University of Illinois Press, Urbane, Illinois.

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

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

SHANNON, C. E., GALLAGER, R. G., AND BERLEKAMP, E. R. (1967), Lower bounds to error probability for coding on discrete memoryless channels. I. *Inform. Control.* **10**, 65–103.

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 Prob. Appl.* (Russian) **10** (1), 167–175.