STRONG CONVERSE OF THE CODING THEOREM FOR SEMICONTINUOUS CHANNELS[1]

BY

J. Wolfowitz

1. Introduction

The purpose of the present paper, which is almost entirely self-contained and requires no prior knowledge of information theory, is to prove the strong converse of the coding theorem for the semicontinuous memoryless channel with any distribution of error whatever (arbitrary noise). The exact result will be stated in Section 4. It will be explained below why it is not possible to reduce our problem by the usual discretization procedure to the discrete memoryless channel, for which the strong converse has been proved. (See Theorem 2 of [1]. Actually this result is stronger than the strong converse; this point will be explained later.) We will also explain below the difference between a weak and strong converse; the two are sometimes confused in the literature.

In [2] and [3] the strong converse of the coding theorem was extended to a certain discrete channel with memory.[2] The proofs rested on the strong converse for the discrete memoryless channel. It is easy to carry over both of these proofs to the analogous semicontinuous channel with memory, provided the strong converse for the semicontinuous memoryless channel has already been proved.

Another proof of the theorem is sketched briefly in the last section. The author is of the opinion that modifications of these proofs will apply to a wide variety of channels.

Professor C. E. Shannon has informed the author that in an unpublished paper he proved the strong converse for the discrete memoryless channel. In [4] he proved the strong converse for a particular continuous channel with additive Gaussian noise.

2. The semicontinuous memoryless channel

We assume, without essential loss of generality, that the alphabet of letters sent or transmitted consists of two symbols, say zero and one. The extension of our results to the case when this alphabet contains any finite number of symbols is trivial.

The channel probability function consists of a pair (because the alphabet of transmitted symbols contains two elements) of probability distribution functions F_0 and F_1. For simplicity of exposition we will take these to be

Received April 16, 1959; received in revised form July 27, 1959.

[1] Research under contract with the Office of Naval Research.

[2] *Added in proof.* The author has since proved the strong converse of the coding theorem for what is called in [10] and [3] the general discrete finite-memory channel.

distribution functions on the real line, although they could be taken to be distribution functions on any σ-algebra of sets without any additional trouble.

In the special case where F_0 and F_1 are step functions on the real line (say) with a finite number of jumps, the channel to be described below is called the discrete memoryless channel (d.m.c.). In the general case it is called the semicontinuous memoryless channel (s-c.m.c.).

Any sequence of n zeros and ones will be called a u-sequence. Any sequence of n real numbers will be called a v-sequence. In our channel u-sequences are sent and are received as v-sequences. If the u-sequence $u = (x_1, \cdots, x_n)$ is sent, the received v-sequence

$$v(u) = (Y_1(u), \cdots, Y_n(u)) \tag{2.1}$$

is a sequence of independent chance variables with distributions given by

$$P\{Y_i(u) < z\} = F_{x_i}(z), \qquad i = 1, \cdots, n, \tag{2.2}$$

where the symbol $P\{\ \}$ denotes the probability of the relation in braces.

A code of length N and probability of error $\leqq \lambda$ is a set

$$\{(u_1, A_1), \cdots, (u_N, A_N)\}, \tag{2.3}$$

where, for $i = 1, \cdots, n$, u_i is a u-sequence, A_i is a Borel set of v-sequences (i.e., A_i, considered as a set of points in n-space, is a Borel set), the A_i are disjoint, and

$$P\{v(u_i) \in A_i\} \geqq 1 - \lambda, \qquad i = 1, \cdots, n. \tag{2.4}$$

Let C be the "capacity" of the channel. This number was first given by Shannon in his fundamental paper [5], and is precisely defined in Section 3 below. Following an initial formulation by Shannon [5], one or more of the following closely related "coding theorems" were proved in [6], [7], [8], and [1], for the d.m.c. and also for other channels:

I. Let $\varepsilon > 0$ and λ, $0 < \lambda \leqq 1$, be arbitrary. For n sufficiently large there exists a code of length

$$N = 2^{n(C-\varepsilon)} \tag{2.5}$$

and probability of error $\leqq \lambda$.

II. Let λ, $0 < \lambda \leqq 1$, be arbitrary. There exists a positive constant $K > 0$ such that, for any n, there exists a code of length

$$N = 2^{nC-Kn^{1/2}} \tag{2.6}$$

and probability of error $\leqq \lambda$.

III. Let $\varepsilon > 0$ be arbitrary. There exist positive constants c_1 and c_2 with the following property: For any n there exists a code of length $2^{n(C-\varepsilon)}$ and probability of error not greater than

$$c_1 e^{-nc_2}. \tag{2.7}$$

These results in the forms I and III can be immediately extended to the s-c.m.c. by the following "discretization" procedure: The real line is divided into a finite number of suitably chosen sets, say $T_1, \cdots, T_k$. When $Y_i(u)$, $i = 1, \cdots, n$, falls into the set T_j, $j = 1, \cdots, k$, it is assigned the value j. In this way the s-c.m.c. is changed to a d.m.c. By proper choice of the sets $\{T_j\}$ one can achieve (this will be obvious from a later argument) that the capacity of the d.m.c. differs by less than any prescribed number from the capacity of the s-c.m.c. The coding theorem for the latter follows at once.[3]

We now return to the d.m.c. To justify the term "capacity" it is necessary also to prove a converse to the coding theorem.

Weak converse of the coding theorem for the d.m.c. Let $\varepsilon > 0$ be arbitrary. Let $\lambda > 0$ be *sufficiently small.* For all n sufficiently large there does not exist a code of length

$$N = 2^{n(C+\varepsilon)} \tag{2.8}$$

and probability of error $\leqq \lambda$.

This theorem was proved in [9] (cited in [10], p. 44). The proof applies to a very large class of channels.

Strong converse of the coding theorem for the d.m.c. Let $\varepsilon > 0$ and λ, $0 \leqq \lambda < 1$, be arbitrary. For n sufficiently large there does not exist a code of length

$$N = 2^{n(C+\varepsilon)} \tag{2.9}$$

and probability of error $\leqq \lambda$.

The basic difference between the two converses may be explained as follows: It is obvious that, essentially, the smaller λ the larger must the A_i be, and the larger λ the smaller may the A_i be. The weak converse says that, if λ is sufficiently small and hence the A_i are sufficiently large, N of the latter cannot be packed into the space of v-sequences. The strong converse says that, no matter how large λ is and hence how small the A_i may be, it is still not possible to pack N of the latter into the space of v-sequences.

The following somewhat stronger form of the strong converse for the d.m.c. was proved in [1]: Let λ, $0 \leqq \lambda < 1$, be arbitrary. There exists a positive constant K' such that, for any n, there does not exist a code of length

$$N = 2^{nC+K'n^{1/2}} \tag{2.10}$$

and probability of error $\leqq \lambda$.

(Professor Lionel Weiss has recently proved that, for a binary symmetric channel (definition in [10], for example) under certain restrictions, the con-

[3] The coding theorem could also be proved directly without discretization by the methods of [6] and [8].

stant K' above can be negative. This stronger (for this particular case) result can be extended to binary almost symmetric channels.[4])

(The strong and weak converses are sometimes confused. Thus, the claim of the authors of [11] that their results contain all previous results is based on such a confusion and is therefore without basis in fact. Actually, [11] repeats the proof of the weak converse given in [9] and [10].)

The strong converse of the coding theorem for the d.m.c. cannot be immediately extended to the s-c.m.c. by the simple discretization procedure which sufficed for the coding theorem, for the following reason: Discretization means that the Borel sets A_i have a particular structure and are not the most general possible. For the A_i of the special form implied by any particular discretization, the strong converse holds at once (even the stronger converse (2.10)). But this alone does not eliminate the possibility that codes might be longer if the A_i were allowed to have their most general form. To put it more graphically and intuitively: It is impossible to pack more than a certain number of the A_i into the space of received sequences when the A_i have a certain "reasonable" shape. But might it not be possible to pack more into the space if the A_i were sufficiently sinuous and tortuous?

Since a discrete channel is also semicontinuous, it might be thought that the result of the present paper implies the strong converse of [1]. This is not so, for the following reason: For the discrete channel the theorem was proved in the stronger form (2.10), while for the semicontinuous channel we are able to prove only the weaker form (2.9). The obstacle to proving the stronger form by the proof which follows is that one has to approximate certain integrals by finite sums.

To within the difference between (2.9) and (2.10) the present result for semicontinuous channels implies the corresponding result for discrete channels. If the functions f_0 and f_1 below (Section 3) are simple, i.e., take only finitely many values, one can, just as in [1], prove the results (2.10). However, this generality is really spurious, because it will be seen that such a channel is essentially discrete and only seemingly semicontinuous.

3. Preliminaries

Let

$$u = (x_1, \cdots, x_n)$$

be the general designation of the u-sequence sent. For purposes only of mathematical manipulation it will frequently be convenient below to assume that the x_i are independent, identically distributed chance variables, with

$$P\{x_i = 1\} = \pi_1 = 1 - P\{x_i = 0\} = 1 - \pi_0 .$$

[4] The proof of the latter result is simply that, by the argument of Theorem 2 of [1], the constant K' is a continuous function of the channel probability function. Professor Weiss's result will be published in the Quarterly of Applied Mathematics.

For brevity we shall describe this as "stochastic input (π_0, π_1)." We invite the reader to verify that the use of this device will in no way vitiate the proof of the theorem stated below. We shall always write below as if $\pi_0 + \pi_1 = 1$, without further definition.

Throughout this paper all logarithms will be to the base 2. (This is purely a matter of convention, as is the fact that the bounds for the length of a code are expressed as powers of 2.) Whenever, in the formulae below, 0 log 0 occurs formally, it is to be understood as zero.

Let μ be the probability measure defined for every Borel set as the sum of the measures assigned to this set by F_0 and F_1. Let f_0 and f_1 be, respectively, Radon-Nikodym derivatives of F_0 and F_1 with respect to μ. Of course these are determined only to within sets of μ-measure zero. However, we shall write below as if they were completely determined and invite the reader to verify that no error will be caused thereby. Thus, we assume $f_0 + f_1 \equiv 1$, and when $u_0 = (a_1, \cdots, a_n)$ is a u-sequence and $v_0 = (b_1, \cdots, b_n)$ is a v-sequence, we write

$$p(v_0 \mid u_0) = \textstyle\prod_{i=1}^{n} f_{a_i}(b_i) \tag{3.1}$$

as the density of $v(u_0)$ at v_0. If also there is a stochastic input, say (π_0, π_1), we write

$$p(u_0) = P\{u = u_0\}, \tag{3.2}$$

$$p(u_0, v_0) = p(u_0)p(v_0 \mid u_0), \tag{3.3}$$

$$p(v_0) = \textstyle\sum_{\text{all } u\text{-sequences}} p(\bar{u})p(v_0 \mid \bar{u}). \tag{3.4}$$

Finally, if A is a Borel set of v-sequences, we write

$$p(A \mid u_0) = \int_A p(\bar{v} \mid u_0)\mu^{(n)}(d\bar{v}), \tag{3.5}$$

where $\mu^{(n)}$ is the product measure $\mu \times \mu \times \cdots \times \mu$ in n-space, and

$$p(u_0, A) = p(u_0)p(A \mid u_0), \tag{3.6}$$

$$p(A) = \sum_{\text{all } u\text{-sequences}} p(\bar{u}, A) = \int_A p(\bar{v})\mu^{(n)}(d\bar{v}). \tag{3.7}$$

This is the notation used in [10] and is completely satisfactory as long as one keeps in mind what the argument of p is, and what, if anything, the stochastic input is. (The expressions $p(v_0 \mid u_0)$ and $p(A \mid u_0)$ do not involve any stochastic input.)

When there is a stochastic input (π_0, π_1), the entropy $H(X)$ of the input has been defined by Shannon [5] as

$$H(X) = -\sum_{i=0}^{1} \pi_i \log \pi_i ; \tag{3.8}$$

the conditional entropy $H(Y \mid X)$ of the output, given the input, as

$$H(Y \mid X) = -\sum_{i=0}^{1} \pi_i \int_{-\infty}^{\infty} f_i(b) \log f_i(b) \mu(db); \tag{3.9}$$

the conditional entropy $H(X \mid Y)$ of the input, given the output, as

$$H(X \mid Y) = -\sum_{i=0}^{1} \pi_i \int_{-\infty}^{\infty} f_i(b) \log \left(\frac{\pi_i f_i(b)}{\pi_0 f_0(b) + \pi_1 f_1(b)} \right) \mu(db); \tag{3.10}$$

and the entropy $H(Y)$ of the output as

$$H(Y) = -\int_{-\infty}^{\infty} \left(\sum_{i=0}^{1} \pi_i f_i(b) \right) \log \left(\sum_{i=0}^{1} \pi_i f_i(b) \right) \mu(db). \tag{3.11}$$

All of these can be shown to be finite. One verifies easily that

$$H(X) - H(X \mid Y) = H(Y) - H(Y \mid X). \tag{3.12}$$

The maximum of the latter with respect to the stochastic input (π_0, π_1) has been called by Shannon [5] the capacity C of the s-c.m.c.

Let $\delta_1 > 0$ be a small number to be determined later. A u-sequence will be called a qu-sequence if the proportion of ones in the sequence differs from q by not more than δ_1 in absolute value.

Let $J_1, \cdots, J_r$ be a set of r disjoint Borel sets whose union is the real line; the sets $\{J_j\}$ will be described in Section 5. We define g_{ij}, $i = 0, 1$; $j = 1, \cdots, r$, by

$$g_{ij} = \int_{J_j} f_i(b) \mu(db). \tag{3.13}$$

Let $N(i \mid u_0)$, $i = 0, 1$, be the number of elements i in the u-sequence u_0. Let $N(i, j \mid u_0, v_0)$, where $i = 0, 1$, $j = 1, \cdots, r$, and u_0 and v_0 are, respectively, a u-sequence and a v-sequence, be the number of integers k, $1 \leqq k \leqq n$, such that the k^{th} element of u_0 is i and the k^{th} element of v_0 lies in J_j.

Let δ_2 and δ_3 be small positive numbers to be determined later. A v-sequence v_0 will be said to be generated (π_1) by a u-sequence u_0 if both the following conditions are fulfilled (only the second condition involves π_1):

$$| N(i, j \mid u_0, v_0) - N(i \mid u_0) g_{ij} | \leqq n\delta_2 g_{ij}, \qquad i = 0, 1; \; j = 1, \cdots, r, \tag{3.14}$$

$$p(v_0 \mid u_0) < 2^{-n(H(Y|X)-\delta_3)}, \tag{3.15}$$

where $H(Y \mid X)$ is computed with the stochastic input (π_0, π_1).

Let π_1, δ_2, δ_3, δ_4 be any positive numbers, with $\pi_1 < 1$. Let δ_1 be sufficiently small and n sufficiently large. From the law of large numbers it follows that, if u_0 is any π_1 u-sequence (i.e., a qu-sequence with $q = \pi_1$),

$$P\{v(u_0) \text{ is generated } (\pi_1) \text{ by } u_0\} > 1 - \delta_4. \tag{3.16}$$

Let d, $0 < d < \frac{1}{2}$, be any fixed number. Later we shall choose a particular d. We shall temporarily assume the truth of the following lemma which will be proved in Section 5.

LEMMA 1. *Let (π_0, π_1) be a stochastic input for which $d \leqq \pi_1 \leqq 1 - d$. Let $\varepsilon > 0$ be arbitrary. Let δ_1 and δ_2 be sufficiently small and n sufficiently large. For any v-sequence v_0 which is generated (π_1) by any π_1 u-sequence we have*

$$p(v_0) > 2^{-n(H(Y)+\varepsilon/8)}. \tag{3.17}$$

4. The strong converse for the semicontinuous channel without memory

We now prove the strong converse for the s-c.m.c.

THEOREM. *Let λ and ε be arbitrary numbers subject only to the conditions $\varepsilon > 0$, $0 \leqq \lambda < 1$. For n sufficiently large there does not exist a code of length $2^{n(C+\varepsilon)}$ and probability of error $\leqq \lambda$.*

If $C = 0$, which happens when and only when $f_0 = f_1$ (almost everywhere (μ)), the theorem is trivial. For then it is impossible to infer anything about the sequence sent from the sequence received. We therefore assume that $C > 0$. Similarly, to avoid the trivial, we assume $\lambda > 0$. The proof of the theorem will be conducted in several lemmas. Lemma 1 has already been given. Hereafter by a code we always mean a code with probability of error $\leqq \lambda$.

LEMMA 2. *Let ε and π_1 be arbitrary positive numbers, with $d \leqq \pi_1 \leqq 1 - d$. Let δ_3 be less than $\varepsilon/8$, and let δ_1 and δ_2 be small enough for Lemma 1 to hold. Let $\{(u_1, A_1), \cdots, (u_N, A_N)\}$ be any code such that $u_1, \cdots, u_N$ are π_1 u-sequences and A_i, $i = 1, \cdots, N$, contains only v-sequences generated (π_1) by u_i. Then, for n sufficiently large,*

$$N < 2^{n(C+\varepsilon/2)}. \tag{4.1}$$

(In (3.16), δ_4 is arbitrary and may be chosen less than λ. Then, if δ_1 is sufficiently small and n is sufficiently large, there exist codes which satisfy the conditions of the lemma.)

Proof. Let n be sufficiently large for Lemma 1 to hold. Let v_0 be any sequence in A_i, $i = 1, \cdots, N$. Then, by Lemma 1 and the definition of a v-sequence generated (π_1) by a u-sequence, we have, for the stochastic input (π_0, π_1),

$$\frac{p(v_0 \mid u_i)}{p(v_0)} < \frac{2^{-n(H(Y|X)-\varepsilon/8)}}{2^{-n(H(Y)+\varepsilon/8)}}, \tag{4.2}$$

so that

$$p(v_0 \mid u_i) < 2^{n(C+\varepsilon/4)}p(v_0). \tag{4.3}$$

Integrating over A_i with respect to $\mu^{(n)}(dv_0)$, we obtain from (4.3)

$$p(A_i \mid u_i) \leqq 2^{n(C+\varepsilon/4)}p(A_i). \tag{4.4}$$

The left member of (4.4) is $\geqq 1 - \lambda$, since (u_i, A_i) is an element of a code. Hence

$$(4.5) \qquad p(A_i) \geqq (1 - \lambda)2^{-n(C+\varepsilon/4)} > 2^{-n(C+\varepsilon/2)}$$

for n sufficiently large and $i = 1, \cdots, N$.

From (4.5) and the fact that the A_i are disjoint, we obtain

$$(4.6) \qquad N2^{-n(C+\varepsilon/2)} < \textstyle\sum_i p(A_i) \leqq 1,$$

so that

$$(4.7) \qquad N < 2^{n(C+\varepsilon/2)}.$$

This proves the lemma.

LEMMA 3. *The conclusion of Lemma 2 holds even if one omits from its hypotheses the requirement that each A_i contain only v-sequences generated (π_1) by u_i, provided that δ_1 is sufficiently small.*

Proof. Let k be so large that $\lambda(1 + 1/k) < 1$. Let δ_3 be any positive number less than $\varepsilon/8$. Let δ_1 be small enough and n large enough for δ_4 of (3.16) to be less than λ/k. Let δ_1 and δ_2 also be small enough for Lemma 1 to hold.

From $A_1, \cdots, A_N$ delete all sequences not generated (π_1) by their respective u_i, and call the results $A'_1, \cdots, A'_N$. Clearly the A'_i are disjoint Borel sets in n-space. From (3.16) it follows that

$$(4.8) \qquad P\{v(u_i) \in A'_i\} > 1 - \lambda - \lambda/k.$$

Hence $\{(u_1, A'_1), \cdots, (u_N, A'_N)\}$ is a code with probability of error $\leqq \lambda(1 + 1/k)$. To this code the conclusion of Lemma 2 applies, since the right member of (4.1) does not involve λ. (The lower bound on n, required in the present lemma, may be higher than that in Lemma 2.)

Proof of the theorem. Let $d > 0$ be such that, for n sufficiently large, the total number of u-sequences in which the proportion of zeros or ones is $\leqq d$, is less than 2^{nC}. Since $C > 0$, this is surely possible.

Let t be any point in the closed interval $[d, (1 - d)]$. Let $\delta_1(t)$ and $n(t)$ be such that, for $\pi_1 = t$, $n > n(t)$, and $\delta_1 = \delta_1(t)$, Lemma 3 holds. To t make correspond the interval $[t - \delta_1(t), t + \delta_1(t)]$. A finite number of such intervals suffices to cover the closed interval $[d, (1 - d)]$; let $t_1, \cdots, t_h$ be their centers.

Let $\{(u_1, A_1), \cdots, (u_N, A_N)\}$ be any code. It may be divided into (not necessarily disjoint) subcodes $K_0, K_1, \cdots, K_h$ in the following way: The u-sequences of the code K_i, $i = 1, \cdots, h$, are all t_i u-sequences.[5] The u-sequences of the subcode K_0 all either have fewer than nd ones or have fewer than nd zeros. By Lemma 3 the length of each subcode K_i, $i = 1, \cdots, h$,

[5] Of course, for each i, δ_1 is $\delta_1(t_i)$.

is less than $2^{n(C+\varepsilon/2)}$ for $n > n(t_i)$. By the choice of d the length of K_0 is less than 2^{nC} for $n > n_0$, say. Hence for $n > \max (n_0, n(t_i), i = 1, \cdots, h)$, we have

$$N < (h + 1)2^{n(C+\varepsilon/2)}. \tag{4.9}$$

For n sufficiently large the right member of (4.9) is smaller than $2^{n(C+\varepsilon)}$, which proves the theorem.

(Actually Lemmas 1, 2, and 3 are valid uniformly in π_1 in the closed interval $[d, (1 - d)]$. To spare the reader any uneasiness on this score we proceeded as above, using the Heine-Borel theorem.)

5. Proof of Lemma 1

We begin by describing the system of sets $J(j), j = 1, \cdots, r$. Let $\delta_5 > 0$ be a small number to be determined later, and

$$0 = c_0 < c_1 < c_2 < \cdots < c_{r-1} < c_r = 1$$

numbers to be chosen in a moment, with $c_1 = 1 - c_{r-1}$. We define

$$J(j) = \{b : c_{j-1} \leqq f_0(b) < c_j\}, \qquad j = 1, \cdots, r - 1,$$
$$J(r) = \{b : c_{r-1} \leqq f_0(b) \leqq c_r\}.$$

We require that the c's be such that the following conditions are fulfilled:

$$\left| \int_{-\infty}^{\infty} f_0(b) \log f_0(b) \mu(db) - g_{01} \log (1 - c_1) - \sum_{j=2}^{r} g_{0j} \log c_{j-1} \right| < \delta_5, \tag{5.1}$$

$$\left| \int_{-\infty}^{\infty} f_1(b) \log f_1(b) \mu(db) - g_{1r} \log (1 - c_1) - \sum_{j=1}^{r-1} g_{1j} \log (1 - c_j) \right| < \delta_5, \tag{5.2}$$

$$g_{01} + g_{1r} < \delta_5, \tag{5.3}$$

and

$$\left| \int_{-\infty}^{\infty} f_i(b) \log \left(\frac{\pi_i f_i(b)}{\pi_0 f_0(b) + \pi_1 f_1(b)} \right) \mu(db) - \sum_{j=2}^{r-1} g_{ij} \log \left(\frac{\pi_i g_{ij}}{\pi_0 g_{0j} + \pi_1 g_{1j}} \right) \right| < \delta_5 \tag{5.4}$$

for $i = 0, 1$ and any (π_0, π_1) such that $\min (\pi_0, \pi_1) \geqq d$. It is easy to see that one can choose the c's so as to meet all of the above conditions.

Let v_0 be a v-sequence which is generated (π_1) by the π_1 u-sequence u_0, with $\min (\pi_0, \pi_1) \geqq d$. In what follows the θ's are always numbers $\leqq 1$ in absolute value. The number of elements i, $i = 0, 1$, in u_0 is

$$n(\pi_i + \theta_i \delta_1) \qquad (\textstyle\sum_i \theta_i = 0).$$

The number of elements of v_0 in the set $J(j)$, $j = 1, \cdots, r$, is therefore

$$h_j = n[(\pi_0 + \theta_0\,\delta_1)g_{0j} + \theta_{0j}\,\delta_2\,g_{0j} + (\pi_1 + \theta_1\,\delta_1)g_{1j} + \theta_{1j}\,\delta_2\,g_{1j}] \qquad (\textstyle\sum_j \theta_{ij}\,g_{ij} = 0, \quad i = 0, 1). \tag{5.5}$$

Let $\bar{U}$ be the totality of all u-sequences $\bar{u}$ which fulfill the following requirements:

$$N(0, 1 \mid \bar{u}, v_0) = 0, \tag{5.6}$$

$$N(1, 1 \mid \bar{u}, v_0) = h_1, \tag{5.7}$$

$$N(0, r \mid \bar{u}, v_0) = h_r, \tag{5.8}$$

$$N(1, r \mid \bar{u}, v_0) = 0, \tag{5.9}$$

$$N(i, j \mid \bar{u}, v_0) = \frac{h_j(\pi_i\,g_{ij})(1 + \theta'_{ij}\,\delta_6)}{\pi_0\,g_{0j} + \pi_1\,g_{1j}}, \quad i = 0, 1;\ j = 2, \cdots, (r - 1), \tag{5.10}$$

where $\delta_6 > 0$ will be determined shortly and

$$\theta'_{0j}\,\pi_0\,g_{0j} + \theta'_{1j}\,\pi_1\,g_{1j} = 0 \tag{5.11}$$

for all j. For any $\bar{u}$ in $\bar{U}$ we have

$$\begin{aligned} \log p(v_0 \mid \bar{u}) &\geqq (h_1 + h_r)\log(1 - c_1) \\ &\quad + \sum_{j=2}^{r-1} \frac{h_j}{\pi_0\,g_{0j} + \pi_1\,g_{1j}}\,[\pi_0\,g_{0j}(1 + \theta'_{0j}\,\delta_6)\log c_{j-1} \\ &\qquad + \pi_1\,g_{1j}(1 + \theta'_{1j}\,\delta_6)\log(1 - c_j)] \\ &\geqq n(1 + \delta_7)\left\{\pi_0\left[g_{01}\log(1 - c_1) + \sum_{j=2}^{r} g_{0j}\log c_{j-1}\right]\right. \\ &\qquad \left. + \pi_1\left[\sum_{j=1}^{r-1} g_{1j}\log(1 - c_j) + g_{1r}\log(1 - c_1)\right]\right\} \\ &> n(1 + \delta_7)(-H(Y \mid X) - \delta_5) \\ &> n(-H(Y \mid X) - \delta_8), \end{aligned} \tag{5.12}$$

where $\delta_8 > 0$ approaches zero as δ_1, δ_2, δ_5, and δ_6 approach zero.

We now obtain a lower bound on the number L of u-sequences in $\bar{U}$. For typographical simplicity write $l_{ij}(\theta'_{ij})$ for the right member of (5.10). We have

$$L = \prod_{j=2}^{r-1} \sum \binom{h_j}{l_{0j}(\theta'_{0j})} \tag{5.13}$$

where the summation is with respect to all θ'_{0j} for which $l_{0j}(\theta'_{0j})$ is an integer. For a $\delta_9 > 0$ which approaches zero as δ_6 approaches zero, we have

$$\begin{aligned} L > &\left[\prod_{j=2}^{r-1} \sum \left\{ \binom{h_j}{l_{0j}(\theta'_{0j})} \prod_{i=0}^{1} \left(\frac{\pi_i\,g_{ij}}{\pi_0\,g_{0j} + \pi_1\,g_{1j}}\right)^{l_{ij}(\theta'_{ij})} \right\}\right] \\ &\times \left[\prod_{j=2}^{r-1} \prod_{i=0}^{1} \left(\frac{\pi_i\,g_{ij}}{\pi_0\,g_{0j} + \pi_1\,g_{1j}}\right)^{-l_{ij}(0)+n\delta_9}\right]. \end{aligned} \tag{5.14}$$

The quantity in the first square bracket of the right member of (5.14) is, for fixed δ_1, δ_2, and δ_6, and all n sufficiently large, by the law of large numbers for Bernoulli chance variables, bounded below by $\frac{1}{2}$, say. The quantity in the second square bracket of the right member of (5.14) is bounded below by

$$2^{n(H(X\mid Y)-\delta_{10})}, \tag{5.15}$$

where $\delta_{10} > 0$ approaches zero as δ_1, δ_2, δ_5, and δ_6 approach zero.

Finally, for any $\bar{u}$ in $\bar{U}$ we have, from (5.6), (5.7), (5.8), (5.9), and (5.10),

$$\begin{aligned} \log p(\bar{u}) &\geqq n\left(\textstyle\sum_{j=2}^{r} \pi_0\, g_{0j} + 2\delta_1 + 2\delta_2 + \delta_5 + 2\delta_6\right) \log \pi_0 \\ &\qquad + n\left(\textstyle\sum_{j=1}^{r-1} \pi_1\, g_{1j} + 2\delta_1 + 2\delta_2 + \delta_5 + 2\delta_6\right) \log \pi_1 \\ &\geqq -\, n(H(X) + \delta_{11}), \end{aligned} \tag{5.16}$$

where $\delta_{11} > 0$ approaches zero as δ_1, δ_2, δ_5, and δ_6 approach zero.

Now choose δ_1, δ_2, δ_5, and δ_6 so small that

$$2(\delta_8 + \delta_{10} + \delta_{11}) < \varepsilon/8.$$

For all n sufficiently large we then have that

$$\begin{aligned} p(v_0) &\geqq \textstyle\sum_{\bar{u}\epsilon\bar{U}} p(\bar{u})p(v_0 \mid \bar{u}) \\ &> \tfrac{1}{2}\cdot 2^{-n(H(X)+\delta_{11}+H(Y\mid X)+\delta_8-H(X\mid Y)+\delta_{10})} \\ &= \tfrac{1}{2}\cdot 2^{-n(H(Y)+\delta_8+\delta_{10}+\delta_{11})} \\ &> 2^{-n(H(Y)+\varepsilon/8)}. \end{aligned} \tag{5.17}$$

This proves Lemma 1.

(The reader has no doubt noticed that we have not made use of (3.15).)

6. An alternate proof

In this section we briefly sketch an alternate proof of the strong converse of the coding theorem for the s-c.m.c. This proof will apply directly to a large class of channels without requiring the use of such auxiliary devices as are employed in [2] and [3]. The sketch is very brief and makes free use of the combinatorial lemmas of [1].

Transform the real line, say continuously, into the unit interval. Let f_0 and f_1 be densities on this interval with respect to Borel measure. Suppose f_0 and f_1 are bounded above and also bounded below by a positive number. In general this will not be the case, and a passage to the limit will be needed to remove this assumption, which for simplicity we make in this sketch.

Let $\delta > 0$ be sufficiently small (how small will appear later). Divide the unit interval into a finite number of Borel sets $\{T_j\}$ with the following properties:

(a) Let m_{ij} and M_{ij} be, respectively, the minimum and maximum of f_i in T_j. Then $M_{ij} \leqq (1 + \delta)m_{ij}$.

(b) Each set T_j has the same measure t.
The reader will object that the second property cannot always be realized. This is true. We require it only for simplicity, and how to treat the general case will be easy to see.

Define

$$c_{ij} = \int_{T_j} f_i(b)\, db,$$

$$V(T \mid \pi) = -\textstyle\sum_{i,j} \pi_i c_{ij} \log c_{ij},$$

$$W(T \mid \pi) = -\textstyle\sum_j \{(\sum_i \pi_i c_{ij}) \log (\sum_i \pi_i c_{ij})\}.$$

Let u_i be any u-sequence of a code all of whose u-sequences are π_1 u-sequences. (We want to bound the length of such a code. The proof for a general code then proceeds as in Section 4.) By an argument not too different from that of Lemma 3 above, and by employing the combinatorial arguments of [1], one can conclude that A_i', defined as in Lemma 3, lies in a Borel set whose volume is at least

$$t^n \cdot 2^{n(V(T|\pi)-\varepsilon)}.$$

Within this volume the ratio of the maximum density to the minimum density is $\leqq (1 + \delta)^n$. Hence A_i' must occupy a volume no smaller than

$$\alpha \cdot (1 + \delta)^{-n} \cdot t^n \cdot 2^{n(V(T|\pi)-\varepsilon)},$$

where $\alpha > 0$ is a constant.

By a combinatorial argument from [1] one can show that the maximum volume available for all such A_i' together is less than

$$t^n \cdot 2^{n(W(T|\pi)+\varepsilon)}.$$

Hence the length of the code is less than

$$(1/\alpha) \cdot (1 + \delta)^n \cdot 2^{n(W(T|\pi)-V(T|\pi)+2\varepsilon)}.$$

When δ is sufficiently small this gives the desired result.

References

1. J. Wolfowitz, *The coding of messages subject to chance errors*, Illinois J. Math., vol. 1 (1957), pp. 591–606.
2. ———, *The maximum achievable length of an error correcting code*, Illinois J. Math., vol. 2 (1958), pp. 454–458.
3. A. Feinstein, *On the coding theorem and its converse for finite-memory channels*, Information and Control, vol. 2 (1959), pp. 25–44.
4. C. E. Shannon, *Probability of error for optimal codes in a Gaussian channel*, Bell System Tech. J., vol. 38 (1959), pp. 611–655.
5. ———, *A mathematical theory of communication*, Bell System Tech. J., vol. 27 (1948), pp. 379–423, 623–656.
6. A. Feinstein, *A new basic theorem of information theory*, Transactions of the Institute of Radio Engineers, Professional Group on Information Theory, 1954 Symposium on Information Theory, pp. 2–22.

7. ———, *Error bounds in noisy channels without memory*, Institute of Radio Engineers Transactions on Information Theory, published by the Professional Group on Information Theory, vol. IT-1 no. 2 (1955), pp. 13–14.

8. C. E. Shannon, *Certain results in coding theory for noisy channels*, Information and Control, vol. 1 (1957), pp. 6–25.

9. R. M. Fano, *Statistical theory of communications*, Notes on a course given at the Massachusetts Institute of Technology, 1952, 1954.

10. A. Feinstein, *Foundations of information theory*, New York, McGraw-Hill, 1958.

11. D. Blackwell, L. Breiman, and A. J. Thomasian, *Proof of Shannon's transmission theorem for finite-state indecomposable channels*, Ann. Math. Statist., vol. 29 (1958), pp. 1209-1220.

Cornell University
Ithaca, New York