SEQUENTIAL DECODING FOR RELIABLE COMMUNICATION

JOHN McREYNOLDS WOZENCRAFT

Desk Copy Only

TECHNICAL REPORT 325

AUGUST 9, 1957

RESEARCH LABORATORY OF ELECTRONICS
MASSACHUSETTS INSTITUTE OF TECHNOLOGY
CAMBRIDGE, MASSACHUSETTS

The Research Laboratory of Electronics is an interdepartmental laboratory of the Department of Electrical Engineering and the Department of Physics.

The research reported in this document was made possible in part by support extended the Massachusetts Institute of Technology, Research Laboratory of Electronics, jointly by the U. S. Army (Signal Corps), the U. S. Navy (Office of Naval Research), and the U. S. Air Force (Office of Scientific Research, Air Research and Development Command), under Signal Corps Contract DA36-039-sc-64637, Department of the Army Task 3-99-06-108 and Project 3-99-00-100.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

RESEARCH LABORATORY OF ELECTRONICS

Technical Report 325 August 9, 1957

SEQUENTIAL DECODING FOR RELIABLE COMMUNICATION

John McReynolds Wozencraft

This report was reproduced by photo-offset printing from the thesis copy which was submitted to the Department of Electrical Engineering, May 1957, in partial fulfillment of the requirements for the degree of Doctor of Science.

Abstract

Shannon's coding theorem for noisy channels states that it is possible to communicate information, with arbitrarily small error, at any rate of transmission less than the channel capacity. The attainable probability of error has previously been bounded as a function of capacity, transmission rate, and delay. This investigation considers the behavior of a new parameter, the average number of decoding computations. A convolutional encoding and sequential decoding procedure is proposed for the particular case of the binary symmetric channel. With this procedure, the average number of decoding computations per information digit can be constrained to grow less rapidly than the square of the delay. The decoding process converges for constant rates of transmission that are not too close to capacity. Although it has not been possible to prove this rigorously, it appears that the probability of error decreases exponentially with delay, and is essentially optimum for transmission rates near the limit of convergence. It also appears that the sequential decoding technique can be extended to more general channels.

ACKNOWLEDGMENT

The author would like to express his gratitude to Professor Jerome B. Wiesner and the Research Laboratory of Electronics for making the facilities of the Laboratory available for this research; and to Zelda R. Wasserman and Evelyn W. Mack, who computed all of the numerical data.

He is particularly indebted to Professors Peter Elias and Claude E. Shannon for their instruction, guidance, and many helpful suggestions.

Especially, the author extends his thanks to Professor Robert M. Fano, without whose constant inspiration and encouragement this work would neither have been undertaken nor have been completed.

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

Introduction

The structure of human language is sufficiently complex that conversation can take place in spite of considerable amounts of noise and interference. Even if many of the individual words are lost, intelligible communication can continue. In this sense, languages are examples of highly effective error-correcting codes, admirably suited through evolution to the natural needs of man.

When raw data is to be transmitted directly from machine to machine, however, the erroneous reception of even a single element of the signal is likely to change the meaning of a message. Since noise is always present on an electric circuit, some sort of artificial language, or code, is needed. This code should permit communication with any required degree of reliability, and in particular should be suited to the automatic encoding and decoding capabilities of the machines themselves.

The theoretical fact that there exist codes with the desired error behavior has been known for several years. How to implement them without human intervention has not been clear.

This report concerns an investigation of a particular type of coding and decoding which may ultimately prove useful for certain types of channels. The code itself is binary – that is, it uses only two symbols.

The performance of this code is analyzed with respect to a channel known mathematically as the binary symmetric channel, abbreviated BSC. For the BSC, the probability of receiving a symbol in error is independent of the transmitted symbol. Furthermore, the BSC is defined to be without "memory": the probability of error for each symbol is statistically independent of everything that has happened before, or that will happen in the future.

Although binary codes are frequently employed, binary symmetric channels are seldom found. The fact that many circuits are used as binary channels, even though their true nature is quite different, is misleading. As an example, a long-range radioteletype channel is binary if we consider the punched tape input and output to be the only

accessible terminals. Of course, other terminals than these are accessible, and other error-reducing techniques than coding are available. But most important, even were this not true, propagation fading would contradict the BSC condition that errors be statistically independent of each other.

The justification of the work reported here, therefore, lies not so much in its direct and unmodified applicability to physically existing binary symmetric channels, but more in the fact that the BSC is analytically tractable without being trivial. Accordingly, it provides an excellent model for preliminary investigation.

It is hoped that in the future coding theory can be integrated with statistical communication and decision theory into a common body of knowledge, and that this will result in significant technological advances. It will be necessary, however, to avoid simplifying assumptions, with respect to real communication systems, which lead to analytical results that are not valid.

CHAPTER I

THE BINARY SYMMETRIC CHANNEL

1. Definition of the Channel

The problem which we consider in this report is that of communicating with great reliability over a "binary symmetric channel." This is a communication channel for which the alphabet consists of only two symbols: for example, 0 and 1. The transmitter sends a sequence made up of zeros and ones into the channel; the same sequence is delivered to the receiver, except that there is a transition probability $p_0 < \frac{1}{2}$ that each digit is received incorrectly - that is, that a transmitted 0 is received as a 1, and conversely.

The evil gremlin who introduces these changes is very simple-minded indeed: he has no memory, and thus operates upon each new digit of the sequence quite independently. Although destructive, he is not consciously malicious, and is at least statistically predictable.

The binary symmetric channel (abbreviated hereafter as BSC) forms a simple mathematical abstraction of many actual communication situations, such as those involving noisy teletype or pulse code modulation systems. On the other hand, the BSC is clearly no better than an approximation to reality. In electrical communication, it is unquantized signal power that is actually received - not an abstract symbol. Furthermore, the gremlins of nature are usually considerably more sophisticated than the one we presuppose: transmission errors are not necessarily statistically independent, and the

probability of digit error is seldom constant. As a compromise, however, the BSC is close enough to physical reality to be interesting, yet sufficiently far removed therefrom to be tractable.

2. The Communication Problem

The situation with which we are concerned is this: A transmitter is given some binary sequence x of the symbols 0 and 1. We call x the information sequence, and require that it be reproduced exactly at the output of a receiver, with probability arbitrarily close to unity. The transmitter and receiver are connected together only through a binary symmetric channel, for which the transition probability p_o is known.

The information sequence x may be any particular binary sequence whatsoever; in every case, we must be prepared to reproduce it at the receiver output.

In this situation, the transmitter is clearly restricted as to what operations it can perform. The nature of the BSC is such that only binary sequences will pass through the channel. However, the transmitter is completely free to transform or "encode" the original information sequence x into some longer binary sequence s, where s represents the sequence that is actually transmitted.

As it passes through the BSC, some of the digits in the transmitted sequence s may be changed. For each digit independently, the probability that this actually occurs is p_o. The receiver, knowing the channel output and that each digit of this output has probability p_o of being incorrect, must then deduce the original sequence x exactly. We specify that this be accomplished with probability as close to unity as may be desired.

Given a BSC, the communication problem is therefore this: to determine a set of rules whereby any information sequence whatsoever is encoded into a transmitted sequence such that the receiver can uniquely and with arbitrarily high probability redetermine the information sequence in spite of channel perturbations. We are interested not only in specifying how the transmitter generates the signal s (the coding problem), but also in how the receiver deduces x (the decoding problem).

There is at least one easy and obvious solution to this problem. For each digit in x, transmit the appropriate symbol $(2n+1)$ times. Thus an information sequence

$$x = 0\ 1\ 1\ 0\ 1\ \ldots\ldots$$

would correspond, when $n = 2$, to the transmitted sequence

$$s = 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ \ldots\ldots$$

The receiver decodes by majority rule: if $(n+1)$ or more digits in each block of $(2n+1)$ digits are 1's, it prints a 1, and vice versa. Clearly, for a transition probability $p_o < \frac{1}{2}$, the decoding probability of error $P(e)$ approaches zero in the limit as n approaches infinity. The difficulty is that in this limit the rate R_t of transmission of information — that is, the ratio of the number of digits in x to the number of digits in s — also approaches zero. All of these results are in full agreement with what would be expected.

In Shannon's original work on information theory,[1] he proves a very different and general theorem which is not at all what one would expect: for a given channel, it is possible by means of sufficiently inspired (and involved) coding to communicate with a

probability of error smaller than any preassigned value, so long only as the rate of information transmission is less than a maximum value known as the channel capacity C. In the particular case of the BSC,[1] with a transition probability p_o ,

$$C = 1 - H(p_o) \tag{1.1}$$

where

$$q_o = 1 - p_o \tag{1.2}$$

and

$$H(p_o) = - p_o \log p_o - q_o \log q_o \tag{1.3}$$

For convenience, except where otherwise noted, all logarithms throughout this paper are taken to the base 2.*

From Shannon's theorem, we see that it is not necessary (as would appear to be the case from the majority-rule example above) continually to reduce the transmission rate R_t in order to reduce the decoding probability of error towards zero. Instead, for any $R_t < C$, we can hold R_t constant, and need only increase the complexity of the code.

Digital communication is playing an increasingly important role in the technology of modern systems. If English text is to be communicated, the reader can compensate for a few mistakes. On the other hand, direct inter-operation of distant digital computers would require extraordinarily low probabilities of error. This report covers an investigation of the coding, decoding, and error characteristics of a particular class of constant transmission rate codes for the BSC which may prove of interest whenever arbitrarily low communication error probabilities are demanded.

---

* H(p) is known variously as the entropy, or comentropy, function.

CHAPTER II

BLOCK CODING

1. Random Block Codes

Significant insight into the problem of communicating over a binary symmetric channel results from recent work by Shannon[2,3] and Elias[4,5] on block codes. In block coding the transmitter and receiver establish by prearrangement identical code books, or sets of possible transmitted sequences. Let each of these sequences be n_f digits long, and denote the entire code book set by S. Each sequence in S is a possible "message" and may be sent over the channel. If there are $|S|$ of these sequences altogether, then

$$|S| = 2^{n_f R_t} \qquad (\text{for } R_t < 1) \qquad (2.1)$$

is an equation defining the rate of transmission R_t in terms of $|S|$ and n_f. A typical code book set S is illustrated in Fig. 2-1.

Each sequence in S has a specified, numbered location in the code book. Let x_i be the binary number giving the location of sequence s_i. Then each number x_i is $n_f R_t$ digits long.

The communications objective is to designate unequivocally to the receiver any arbitrary binary information sequence x that may be specified to the transmitter. We proceed according to the following rules: Divide the information sequence x into blocks of length $n_f R_t$, and transmit in order the code book sequences s_i corresponding to the resulting string of binary numbers. Each successive block of $n_f R_t$ digits in the original information sequence is thus encoded — and, necessarily, decoded — independently.

The receiver seeks to identify each binary number x_i in turn. Since the channel may introduce transmission errors, in general the received sequence differs in some of its n_f digits from the transmitted sequence s_i. Let y represent the received message. Then the task of the receiver is this: given the set S of all $2^{n_f R_t}$ possible messages, the received sequence y, and advance knowledge of the statistical behavior of the channel, determine which number x_i was designated by the transmitter.

The probability of error is just the probability that the receiver decides incorrectly.

Effect of Noise. For convenience, we may always use the symbol x_o to represent the binary number of length $n_f R_t$ that the transmitter wishes to communicate in any particular instance, and the symbol s_o to represent the corresponding code book sequence of length n_f that is actually transmitted. For a BSC, the perturbing channel noise can also be represented by a binary sequence Ψ_o. If the presence of a 1 in Ψ_o is interpreted to mean that the channel introduces an error in that digit where the 1 appears, then the received sequence y is

$$y = s_o \oplus \Psi_o \qquad (2.2)$$

We use the notation $\oplus$ to mean addition modulo-2 of corresponding digits.

An example is given below.

Transmitted Sequence: $s_o = 1\ 1\ 0\ 0\ 1\ 0\ 0\ \ldots\ldots\ 0$

Noise Sequence: $\Psi_o = 0\ 1\ 0\ 0\ 0\ 1\ 0\ \ldots\ldots\ 1$

$\oplus$

Received Sequence: $y = 1\ 0\ 0\ 0\ 1\ 1\ 0\ \ldots\ldots\ 1$

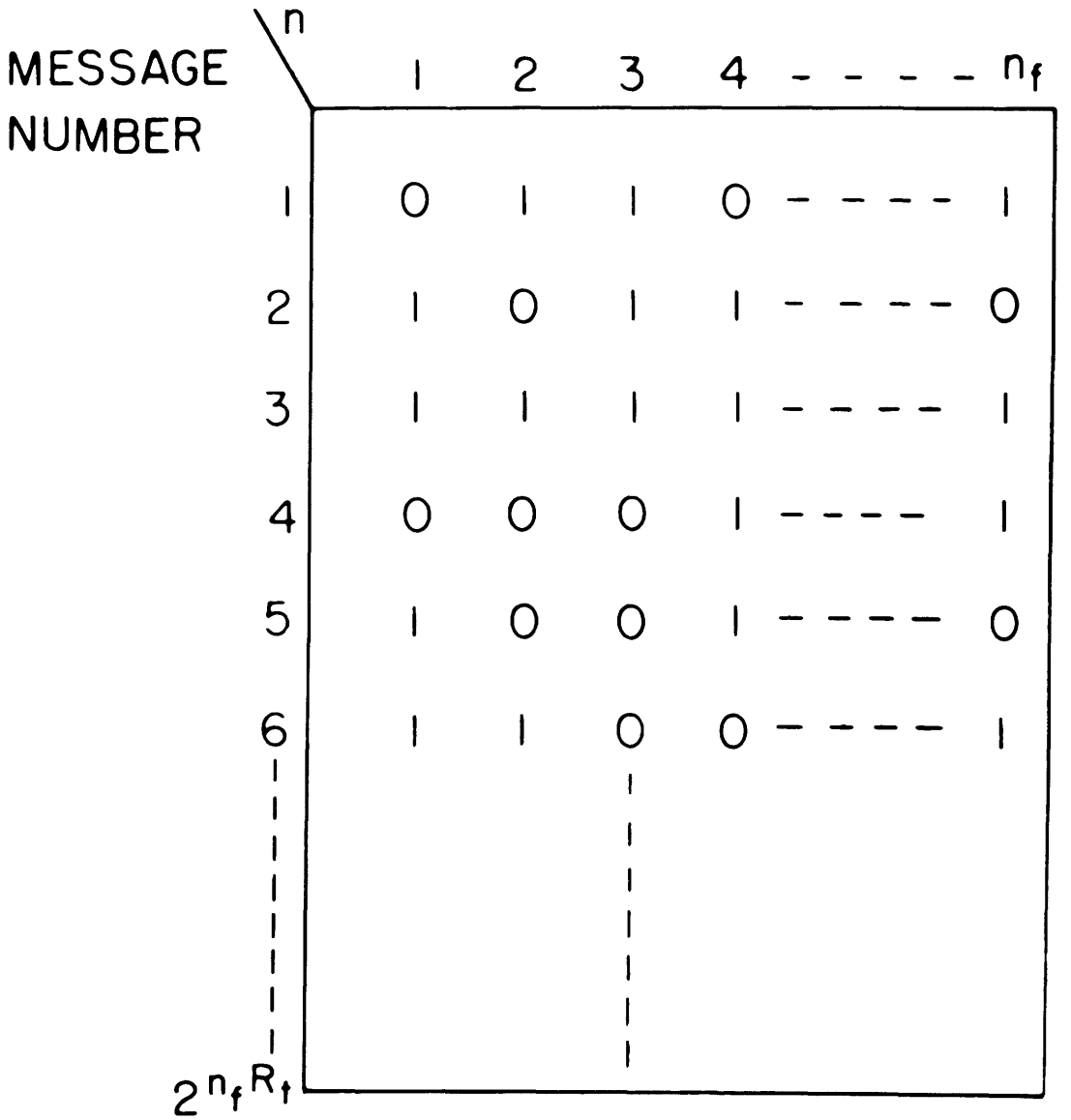

Figure 2-1

BLOCK CODING

Since any binary sequence added modulo-2 to itself gives the identity sequence of all zeros,

$$y \oplus s_o = \Psi_o \tag{2.3}$$

Block Decoding. After having received all n_f digits of the sequence y, the receiver proceeds to decode in accordance with the following rules:

1. The receiver adds y modulo-2 to each sequence s_i in the set S, thereby generating a set of $2^{n_f R_t}$ "noise" sequences Ψ_i.

$$\Psi_i = y \oplus s_i \tag{2.4}$$

2. The receiver then counts the number d_i of 1's in each sequence Ψ_i.

$$d_i = \text{number of 1's in } \Psi_i \tag{2.5}$$

For convenience, we may use Hamming's[6] nomenclature, and refer to d_i as the "distance" separating the two sequences s_i and y. The use of this geometrical terminology is justified in Chapter VI.

3. Finally, the receiver decides that the sequence s_i for which d_i is a minimum corresponds to the binary number which the transmitter sought to communicate.

These decoding rules constitute a maximum-likelihood detection criterion, for any BSC transition probability $p_o < \frac{1}{2}$. This follows from the fact that each sequence Ψ_i is precisely that noise sequence which would have produced the given received sequence y, had s_i been transmitted. The most probable noise sequence, when $p_o < \frac{1}{2}$, is that which contains the smallest number of 1's. If two or more of the possible noise sequences Ψ_i have the same

(minimum) number of 1's, the situation is ambiguous. In this report, we consider such an ambiguity to be an error.

Average Probability of Error. An ordered set S of $2^{n_f R_t}$ sequences, each n_f digits long, can be constructed in $2^{n_f 2^{n_f R_t}}$ ways. The probability of error for any particular choice of S may be difficult to compute. It is instructive, however, to consider the average probability of error behavior, over the ensemble of all possible sets S. This problem has been treated in detail independently by Elias[4,5] and Shannon.[2] The methods and results are summarized briefly below.

According to the specified decoding rules for block coding, the receiver will make an error if, and only if, one or more of the incorrect distances d_i is less than or equal to d_o, where

$$d_o = \text{number of 1's in } \Psi_o \tag{2.6}$$

Assume for purposes of analysis that in a particular experiment exactly k transmission errors occur. With this hypothesis, a decoding error is made if any incorrect sequence s_i in S is such that its distance d_i from the received message is less than or equal to k.

Over the ensemble of all possible message sets S, each of the 2^{n_f} binary sequences of length n_f is equally likely to appear in each of the $2^{n_f R_t}$ numbered positions in S. Averaging over the ensemble of message sets is therefore equivalent to considering the average behavior of a single set, each sequence of which is selected independently at random with replacement from among all of the binary sequences n_f digits long. With this "random coding" model, every

sequence of concern (including the received message y) is then statistically independent of every other sequence.

The ensemble probability that a particular incorrect sequence s_i differs from the received message y in k digits or fewer is therefore[7]

$$P(d_i \leqslant k) = 2^{-n_f} \sum_{j=0}^{k} \binom{n_f}{j} \tag{2.7}$$

where $\binom{n_f}{j}$ is the binomial coefficient. There is a total of $(|S| - 1)$ incorrect messages. The probability that none of them differ from y in k or fewer digits is

$$P(\text{no } d_i \leqslant k) = \left[1 - P(d_i \leqslant k)\right]^{|S|-1} \tag{2.8}$$

Since

$$P(\text{any } d_i \leqslant k) = 1 - P(\text{no } d_i \leqslant k) \tag{2.9}$$

we have finally

$$P(\text{any } d_i \leqslant k) < |S|\ P(d_i \leqslant k) \tag{2.10a}$$

whenever the r.h.s. is less than unity, and

$$P(\text{any } d_i \leqslant k) \leqslant 1 \tag{2.10b}$$

otherwise. Equations (2.10a) and (2.10b) are bounds on the ensemble average probability of error, given k transmission errors. Denoting a conditional probability by a subscript, we have

$$P_k(e) = P(\text{any } d_i \leqslant k) \tag{2.11}$$

In order to find the over-all probability of error, we must next average this conditional probability over the possible transmission error patterns. The probability of exactly k transmission

errors is

$$P(d_o = k) = p_o^k \, q_o^{n_f - k} \binom{n_f}{k} \qquad (2.12)$$

Finally, then, the average probability of error with block coding, over the ensemble of all possible message sets, is equal to

$$P(e)_{random} = \sum_{k=0}^{n_f} P(d_o = k) P(\text{any } d_i \leqslant k) \qquad (2.13)$$

We employ the subscript "random" to indicate the analysis technique used in the calculation.

In Section 2 of Appendix A, a firm upper bound to $P(e)_{random}$ is derived in terms of the channel transition probability p_o and the transmitted sequence length n_f, for information transmission rates R_t less than the channel capacity C.

$$P(e)_{random} < (A_r + A_t) 2^{-n_f E_t} \qquad (\text{for } p_o < p_t < p_{crit}) \qquad (A.54)$$

$$< A_{crit} \, 2^{-n_f E_{crit}} + A_t \, 2^{-n_f E_t} \qquad (\text{for } p_{crit} \leqslant p_t \leqslant \tfrac{1}{2}) \qquad (A.55)$$

In these equations, the auxiliary parameter p_t is defined as the solution to

$$R_t = 1 - H(p_t) \qquad (A.33)$$

and p_{crit} is determined as the solution to

$$\frac{p_{crit}}{q_{crit}} = \sqrt{\frac{p_o}{q_o}} \qquad (\text{where } q_{crit} = 1 - p_{crit},\ q_o = 1 - p_o) \qquad (A.46)$$

When we further define the transmission rate corresponding to $p_t = p_{crit}$ as the critical rate,

$$R_{crit} = 1 - H(p_{crit}) \tag{A.65}$$

then specifying $p_t < p_{crit}$ is equivalent to requiring that R_t be greater than R_{crit}. The significance of this critical rate is discussed in Section 2 of this chapter.

The coefficients in Eqs.(A.54) and (A.55) are given by

$$A_r = \frac{1}{\left(1 - \frac{p_t}{q_t}\right)\left[1 - \frac{q_o}{q_o}\left(\frac{p_t}{q_t}\right)^2\right]} \cdot \frac{1}{2\pi\, n_f p_t q_t} \qquad (\text{where } q_t = 1 - p_t) \tag{A.49}$$

$$A_t = \frac{1}{\sqrt{2\pi\, n_f p_t q_t}} \cdot \frac{p_o q_t}{(p_t - p_o)} \tag{A.50}$$

and

$$A_{crit} = \frac{1}{\left(1 - \frac{p_t}{q_t}\right)} \cdot \frac{p_t}{2\pi\, p_{crit} q_{crit}} \tag{A.51}$$

Lastly, the exponential factor E_t is determined by

$$E_t = H(p_o) - H(p_t) + (p_t - p_o) \log \frac{q_o}{p_o} \tag{A.52}$$

and E_{crit} is defined as the value of E_t when $p_t = p_{crit}$.

The functional characteristics of E_t are most clearly interpreted geometrically, as in Fig. 2-2. A horizontal line drawn at a distance R_t beneath the maximum of the entropy curve intersects it at $H(p_t)$. Since the slope of the line tangent to $H(p)$ at p_o is $\log \frac{q_o}{p_o}$, E_t is the vertical distance from $H(p_t)$ to this tangent.

We are especially interested in the behavior of $P(e)_{random}$ with respect to the code length n_f, for fixed values of C and R_t. The

coefficients A are at worst constant with respect to n_f, and the exponential factors E are functions only of the transmission rate and the channel capacity. Accordingly, $P(e)_{random}$ is bounded by an expression which decreases at least exponentially with length n_f. This is a tremendously powerful result. In order to decrease $P(e)_{random}$ from 10^{-6} to 10^{-12}, for a given channel and a constant information transmission rate, we need at most double the code length n_f.

Recalling that $P(e)_{random}$ is defined as the average decoding probability of error over the ensemble of all block codes, we are certain that at least one such code performs this well. Even more strongly, as Shannon[3] points out, if the average value of a set of positive quantities is P, then at most $1/\rho$ of these quantities can have a value greater than ρP. Accordingly, if n_f is so chosen for a given R_t and C that $P(e)_{random} \leqslant 10^{-12}$, at least 90 per cent of all possible block codes of the same length must have a decoding probability of error which is no greater than 10^{-11}.

The fact that codes exist whereby information can be communicated at a constant rate over a general noisy channel with an arbitrarily small non-zero probability of error was first proved by Shannon.[1] Subsequently, Feinstein[8] demonstrated that this achievable probability of error decreased exponentially with increasing code length. Shannon[2,3] has since obtained for general channels results which are exactly comparable to those given above for the BSC.

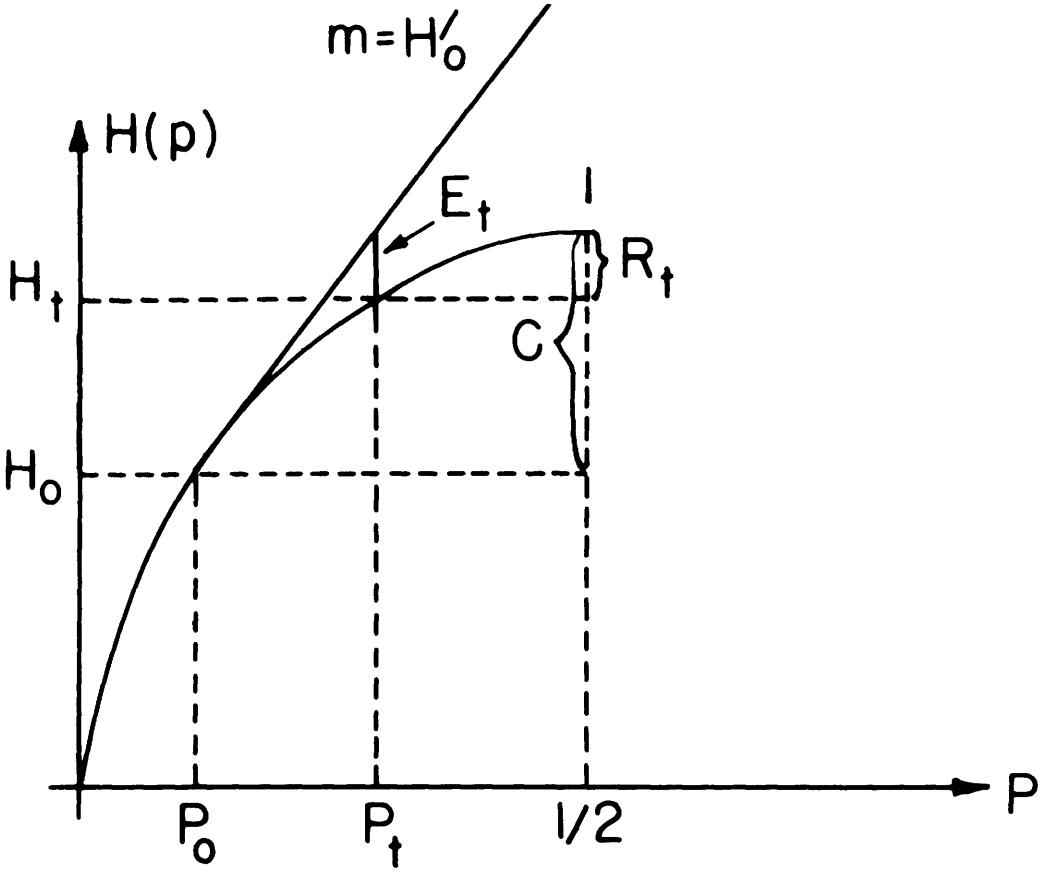

Figure 2-2

GEOMETRIC CONSTRUCTION

H_t means $H(p_t)$

H_o means $H(p_o)$

2. Optimum Block Codes

Except in special cases,[6,9,10] we do not know how to construct an optimum block code — that is, a message set S_{opt} such that the decoding probability of error is minimum for a given channel, block length, and transmission rate. In spite of this fact, however, it is possible to evaluate a quantity $P(e)_{opt}$ which underbounds the lowest probability of error that could possibly be obtained. We again summarize results obtained by Elias.[4,5]

Consider a code book S_{opt} containing $|S|_{opt}$ entries, each n_f digits long. Assume that S_{opt} could be so constructed that any transmission error pattern involving k_1 or fewer digit errors is correctly decoded. Then the receiver must associate with each message s_i in S_{opt} <u>every</u> possible received sequence of length n_f that differs from s_i in k_1 or fewer digits. Furthermore, each of the $|S|_{opt}$ subsets of associated sequences must be disjoint. Since there are only 2^{n_f} possible received sequences, it follows that the number of messages in S_{opt} could be no larger than

$$|S|_{opt} = \frac{2^{n_f}}{\sum_{j=0}^{k_1} \binom{n_f}{j}} \tag{2.14}$$

For this situation, the decoding probability of error $P(e)_{opt}$ would be just the probability that more than k_1 transmission errors occur. Furthermore, it is clear that for a given length n_f no smaller probability of error could ever be obtained with this same number of messages.* This follows from the fact that changing the subset assignment of any one of the possible received sequences

---

* This statement, of course, implies that all possible information sequences x are equally probable.

would associate it with another member of S_{opt} from which it was necessarily more distant, in violation of the maximum-likelihood detection criterion. Accordingly, we have

$$P(e)_{opt} = \sum_{j=k_1+1}^{n_f} p_o^j \, q_o^{n_f-j} \binom{n_f}{j} \tag{2.15}$$

In Section 2 of Appendix A, this expression is evaluated, and it is shown that, asymptotically as n_f goes to infinity,

$$P(e)_{opt} \gtrsim A_{opt} \, 2^{-n_f E_1} \tag{A.62}$$

where (letting $k_1/n_f = p_1 = 1 - q_1$)

$$A_{opt} = \frac{p_o q_1}{q_o p_1} \cdot \frac{1}{\sqrt{8 n_f p_1 q_1}} \tag{A.63}$$

and

$$E_1 = H(p_o) - H(p_1) + (p_1 - p_o) \log \frac{q_o}{p_o} \tag{A.64}$$

The lower bound on $P(e)_{opt}$ given in Eq.(A.62) is strikingly similar to the upper bound on $P(e)_{random}$ given in Eq.(A.54) for rates of transmission greater than critical. In Appendix A we show that in the limit as the code length n_f approaches infinity, $|S|_{opt}$ varies exponentially as $2^{n_f[1-H(p_1)]}$. Since for random block coding we define $|S| = 2^{n_f R_t}$, and $R_t = 1 - H(p_t)$, it follows that for large n_f the parameter p_1 is equivalent to p_t. We therefore have the following powerful result for block coding. In the limit of large code length, the ensemble average probability of error behavior is exponentially optimum, for rates of transmission

R_t greater than critical. Not only are most block codes good, but they are exponentially as good as possible.

This exponential equivalence does not hold true for transmission rates $R_t \leqslant R_{crit}$. For these low rates of transmission, the number of messages $|S|$ is small. With random sequence selection, decoding errors are more likely to be due to a poor choice of message sequences than to the rare occurrence of an improbable noise pattern. We note that it is the term involving E_{crit} that dominates the bound on $P(e)_{random}$ given in Eq.(A.55) for $p_t \geqslant p_{crit}$, which is in accordance with this interpretation. For $R_t > R_{crit}$, on the other hand, the message sequences are so numerous that most decoding errors are attributable to the occurrence of an improbable number of transmission errors.

3. Check Digit Codes

A great deal of the prior work[4,5,6,9,10] done in coding for the BSC concerns a restricted class of block codes known as check digit codes. These codes are most easily described in terms of a coding matrix such as that illustrated in Fig. 2-3. As shown there, the n_{Ch} by n_{Ch} submatrix on the left is diagonal; the remainder of the matrix is filled with n_{Ch} "check patterns" of length n_I.

Each sequence s in the set of possible messages S is composed of n_I arbitrary information digits, followed by n_{Ch} check digits. The total length n_f of any message is therefore equal to $(n_I + n_{Ch})$, and the transmission rate R_t equals $n_I/(n_I + n_{Ch})$.

The transmitted sequence s_o is determined according to the following rules. The n_I information digits are chosen to be the

binary number x_o that we wish to communicate. The check digits which follow are then determined through interaction of x_o and the coding matrix. Let c_{ij} be the j^{th} digit of the check pattern c_i associated with the i^{th} diagonal 1 in the matrix, and let x_{oj} be the j^{th} digit of x_o. We calculate the value s_{oi} of the i^{th} check digit in s_o by the equation

$$s_{oi} = \sum_{j=1}^{n_I} \oplus \; x_{oj} \cdot c_{ij} \qquad (2.16)$$

where the addition is modulo-2. We may think of this operation as the computation of a parity check over a set of digits selected out of x_o by the appropriate check pattern in the coding matrix. As an example, if

$$x_o = 0\ 1\ 0\ 1\ 1\ 0$$

$$c_i = 1\ 1\ 0\ 1\ 0\ 0$$

then

$$s_{oi} = 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 = 0$$

The decoding rules for check digit codes are somewhat more complicated. First of all, the receiver is presumed to have an identical copy of the coding matrix. It then proceeds as follows. Using Eq.(2.16), the decoder calculates on the basis of the received message y what the i^{th} check digit s_{oi} should be, and adds this modulo-2 to the corresponding i^{th} check digit that is actually received. It does this for every value of i, from 1 to n_{Ch}. By doing so, the receiver effectively compiles a list telling which parity checks hold true and which fail.

It is also possible to have compiled a set of such lists in

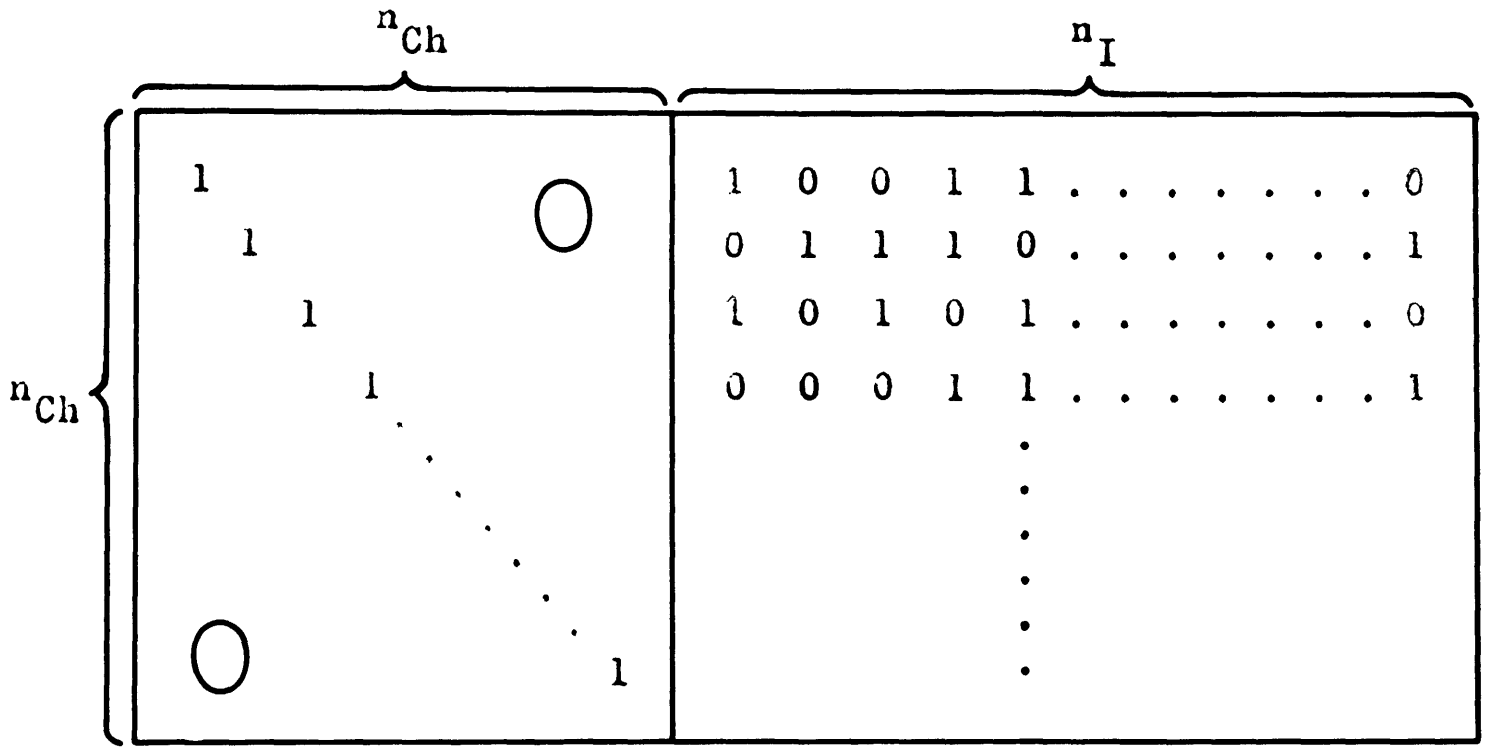

Figure 2-3

RANDOM CHECK DIGIT CODING

advance, detailing for each of the 2^{n_f} possible channel noise sequences Ψ which of the n_{Ch} parity checks will be affected. A maximum-likelihood detection criterion is then to locate the receiver list within the prepared set, and to decide that the actual noise Ψ_o is that particular sequence Ψ, consistent with the observed effect, which involves the smallest number of digit errors. Finally, having determined the most probable channel noise, the receiver corrects the received message, and prints x_o.

With the procedure above, the probability of error is the probability that some Ψ other than Ψ_o, involving no more digit errors, causes an identical list of parity check failures.

Random Check Patterns. Although Hamming,[6] Reed,[9] and Slepian[10] have found specific check digit codes that are optimum in special cases, no general procedure has yet been discovered for determining an optimum matrix for arbitrary transmission rate R_t and length n_f. However, Elias[4] has again proved by means of a random argument that the average probability of error, over the ensemble of all possible ways of filling in the check patterns in the coding matrix, is still given by Eq.(A.54) or (A.55). It is accordingly clear that within the restricted class of all check digit codes are to be found many examples that are at least exponentially optimum.

As a matter of fact, the search for good codes can be narrowed still further without changing this situation. Elias also shows[4] that the random coding bound applies equally well over the ensemble of all check digit codes generated by "sliding" some single binary sequence g of length n_f into the pattern submatrix of Fig. 2-3 —

that is, by writing the first n_I digits of g in the first row, digits 2 to $(n_I + 1)$ in the second row, and so on. It is with a situation closely akin to this that we are concerned in the later chapters of this report. We refer to the sequence g as the check digit generator.

Symmetry. Slepian[10] has proved that for any check digit code, the set S of all possible messages forms an algebraic group, and hence exhibits remarkable properties of symmetry. Consider any two of the 2^{n_I} possible information sequences, x_k and x_ℓ. Then

$$x_k \oplus x_\ell = x_m \tag{2.17}$$

where x_m is also one of the possible information sequences. In order to calculate the i^{th} check digit of the m^{th} message sequence, we use Eq.(2.16).

$$s_{mi} = \sum_{j=1}^{n_I} \oplus \; x_{mj} \cdot c_{ij} \tag{2.18}$$

The operation of addition modulo-2 is distributive. Accordingly,

$$s_{mi} = \left[\sum_{j=1}^{n_I} \oplus \; x_{kj} \cdot c_{ij}\right] \oplus \left[\sum_{j=1}^{n_I} \oplus \; x_{\ell j} \cdot c_{ij}\right] \tag{2.19}$$

or

$$s_{mi} = s_{ki} \oplus s_{\ell i} \tag{2.20}$$

Inasmuch as this result is true for every i, k, and ℓ, it follows that if any two sequences s_k and s_ℓ are members of the set S of all 2^{n_I} possible messages generated by any particular choice of coding matrix, then $s_m = s_k \oplus s_\ell$ is also a member of S. Furthermore, for that information sequence x which has zeros in every digit, the corresponding transmitted message s is itself identically

zero. Lastly, every sequence s_i is its own inverse — that is, $s_i \oplus s_i$ is identically zero. Since the operation "sequence addition modulo-2" is associative and commutative, we therefore find that the message set S for any check digit code satisfies all of the Abelian group requirements,[11] under this operation. Conversely, it can be shown that any group code is a check digit code.

The symmetry property of group (check digit) codes is summarized in the closure statement: The modulo-2 sequence sum of any two members of S is also a member of S. Since every sequence in S is different, this means that if any one sequence is added to every other sequence, the set S is reproduced. Similarly, when some noise sequence Ψ_o is added to a particular member s_o of S during transmission, resulting in a received sequence y, the set of distance measurements d_i formed by adding y to each member of S is invariant with respect to which sequence in the group s_o represents.

The general maximum-likelihood decoding rules given in Section 1 of this chapter involve only this set of distances d_i. Accordingly, as Slepian[10] first pointed out, for group codes the probability of error is independent of which message in the set is actually transmitted. The correctness of this statement is also immediately evident from the special decoding rules for check digit coding. In this case only the effect of the noise upon the n_{Ch} parity checks is significant, and the transmitted information subsequence is not involved at all.

4. The Decoding Problem

Before proceeding, it is helpful to consider briefly the significance of these previously published results. It is possible to communicate, over a binary symmetric channel in particular, with a probability of error which decreases exponentially with increasing code length n_f. Furthermore, this can be achieved while maintaining any constant rate of information transmission less than the channel capacity. In other words, the number of possible messages from which the receiver is able to select the single message actually transmitted increases exponentially with n_f at the same time that the probability of error decreases exponentially.

The maximum-likelihood decoding rules specified for block coding in general, and check digit coding in particular, result in an ensemble average probability of error that is exponentially optimum in the limit of large code-word length n_f, for transmission rates near capacity. Most codes, then, are good codes, and it should not be difficult to find some particular message set S for which the actual probability of error P(e) is as small as may be desired. For a given channel and required transmission rate R_t, we need only determine a sufficiently large code length n_f, select S at random, and avoid being unlucky.

From a strictly practical point of view, however, there remains a serious difficulty. The general block coding procedure involves the storage of a set S of possible messages whose number grows exponentially with n_f, for constant R_t. Since strong statistical assertions require large samples of data, in most interesting cases n_f tends to range from approximately 100 to 600 for values of

$P(e)$ less than 10^{-6}. As an example: $n_f = 150$ and $R_t = 1/5$ implies $|S| = 2^{30} \approx 10^9$, which is already a most unattractively large number. Finally, from a computational point of view, the received message y must be compared in decoding against each of these $|S|$ messages.

Especially when a "sliding" parity check generator sequence is used, check symbol coding avoids the message storage difficulty. However, an exponential problem still exists. The decoding rules in this case require at the receiver a set of lists that in essence equate parity check failures to transmission error patterns. There are n_{Ch} check digits, and therefore $2^{n_{Ch}}$ maximum-likelihood channel error patterns that must be recorded. Since $n_f = n_I + n_{Ch}$, and $R_t = n_I/(n_I + n_{Ch})$, the number of such entries also grows exponentially, as $2^{n_f(1-R_t)}$.

The only practicable code discussed in the literature so far that permits communication over a BSC at a positive rate with arbitrarily small error probability is due to Elias.[12] This is an iterative Hamming[6] technique, in which each information digit enters into an increasing number of parity checks as the transmission continues. Although the probability of error for iterated coding does not decrease so fast with increasing message length n_f as is theoretically possible, the existence of at least one feasible error-free procedure is encouraging. Otherwise, the frustrating knowledge that the ensemble average of all codes is exponentially optimum might lead us to infer that only those codes of which one cannot think are good.

With this introduction, the remaining chapters of this report consider a coding and decoding procedure that seeks to retain the exponentially optimum probability-of-error advantages of block coding, while avoiding the disadvantages of exponential growth in storage and computation requirements.

CHAPTER III

CONVOLUTIONAL ENCODING

1. The Code Book Structure

As mentioned in Chapter II, Elias[4] has shown that the average probability of error behavior of "sliding" check digit codes, over the ensemble of all 2^{n_f} possible check digit generator sequences g, is exponentially optimum. For this technique, encoding is not a problem. Given any particular check digit generator sequence g, and an information sequence x_o, a digital computer can determine the appropriate transmitted sequence s_o in a straightforward fashion. Furthermore, the encoding computer can be small; only the information sequence x_o, the generator g, and s_o need be stored in the computer memory. As a matter of fact, given enough time, this same computer could generate the entire code book set S of all possible messages, one after the other.

All of the above statements apply with equal force to another method of check digit coding which was first considered from a somewhat different point of view by Elias.[4] This technique, convolutional coding, results in a set S of possible messages having a structure of the type illustrated in Fig. 3-1.

This structure is tree-like, in that at each length $n = n_o$, $2n_o$, $3n_o$ ..... , and so forth, there is a node, out of which diverge $2^{n_o R_t}$ branches of length n_o. Since the BSC is discrete, n_o and R_t are subject to the diophantine constraint that $n_o R_t$ must be an integer. For the case illustrated, $n_o = 3$ and $R_t = 1/3$. Consider a convolutional set S of messages $n = (n_o$ times an integer)

digits long. Then there are exactly 2^{nR_t} possible messages in S. We adopt the usual convention that the information sequence x_i corresponding to the message sequence s_i is the binary number of length nR_t that designates the location of s_i in the set. As an example, for the set shown in Fig. 3-1, in order to communicate the number

$$x_{13} = 1\ 1\ 0\ 1$$

the message actually transmitted is

$$s_{13} = 0\ 1\ \underline{1}\ 1\ 1\ \underline{1}\ 0\ 1\ \underline{0}\ 0\ 0\ \underline{1}$$

The situation here is not the same as in the case of block coding, however. There the information sequence x_o is subdivided into blocks of length $n_f R_t$ for coding purposes, and each block is treated separately. In convolutional coding, on the other hand, the code book tree set S continues to grow exponentially as the length of the information sequence increases indefinitely.

This tree-structure of S forces a change in the decoding philosophy. Instead of receiving a sequence y that is n_f digits long and decoding it all at once, with convolutional coding we determine the value of each successive information digit in turn. The receiver accomplishes this by means of distance measurements between S and the next n_f as yet undecoded digits in y. This still implies, of course, that the receiver operates with a time lag of at least n_f digits behind the transmitter. In order to make the decoding problem homogeneous from digit to digit, we require that the decoding observation span n_f equal an integral number of branch lengths n_o. This, of course, is a convenience rather than a necessity.

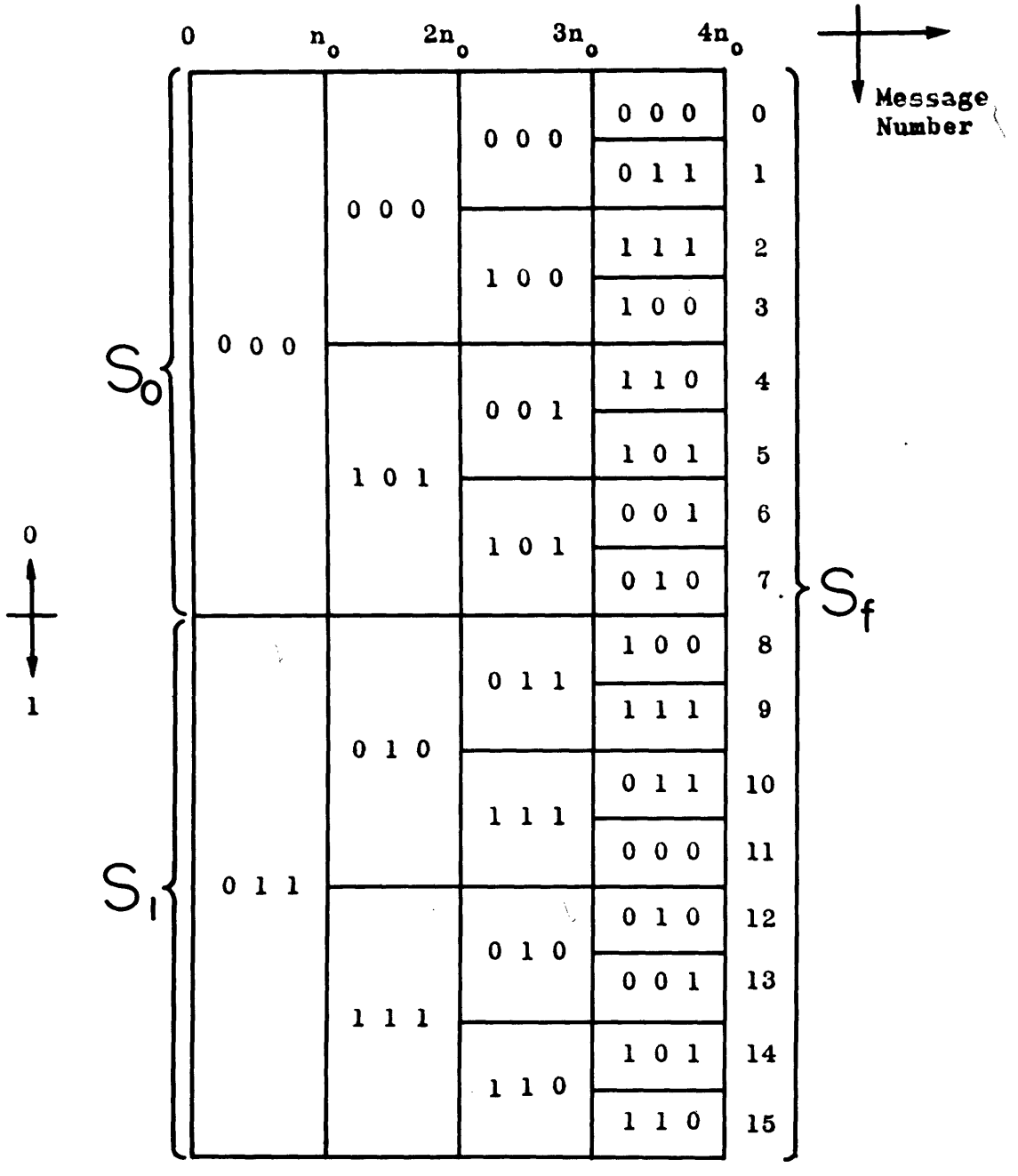

Figure 3-1

CONVOLUTIONAL MESSAGE SET

It is with a decoding procedure for these convolutional codes that this report is concerned. Before this subject is discussed further, however, it is advisable to consider the encoding technique in detail.

2. Convolutional Encoding Constraints

The mechanical analogue of a convolutional encoding computer is illustrated in Fig. 3-2. A check digit generator sequence g, n_f digits long, is arranged around the periphery of a wheel. As shown in the figure, there is a "window" $n_f R_t$ digits long at the top of the wheel, which we can think of as selecting a segment of the generator sequence g. The wheel rotates counterclockwise through the window in unit steps.

The information sequence x_o also passes through the window, in unit steps from left to right. Before communication begins, the information digits within the window are assumed to be all zeros, and the wheel itself is assumed to be resting in a preassigned starting position.

The stepping of x_o and g is controlled according to the following convention. Before each of the first $n_o R_t$ digits in s_o is generated, the information sequence x_o steps once from left to right, and g holds still. Before each of the next $n_o(1-R_t)$ digits, the generator g steps once counterclockwise, and x_o holds still. After each small block of n_o digits, this convention repeats itself. For convenience, we refer to the first $n_o R_t$ digits in a block as "information" digits, and to the last $n_o(1-R_t)$ digits as "check" digits.

The value of the digits that actually make up the transmitted sequence s_o are determined by means of Eq.(3.1) below. Let x_{oj} represent the information symbol that is located in the j^{th} position under the window, and let g_{ij} represent the check digit generator symbol located directly beneath x_{oj}. The subscript i in g_{ij} signifies that the encoding mechanism is properly positioned to compute the i^{th} digit s_{oi} of the transmitted sequence s_o. Then s_{oi} is determined by the equation

$$s_{oi} = \sum_{j=1}^{n_f R_t} \oplus \; x_{oj} \cdot g_{ij} \qquad (3.1)$$

As in the corresponding Eq.(2.16) for check digit block coding, the summation is modulo-2.

As a matter of fact, Eq.(3.1) is exactly equivalent to Eq. (2.16). It therefore follows directly from the symmetry arguments in Section 3 of Chapter II that the entire convolutional set S of any length n is also an Abelian group under the operation of sequence addition modulo-2.

3. Characteristics of Convolutional Message Sets

There are a number of characteristics possessed by every convolutional code set S that are of particular importance in decoding. First of all is the fact that the total number of possible sequences $|S|$ at any length n is approximately equal to 2^{nR_t}. This is not an exact equality, since the tree-structure of S branches only at a discrete set of node points. However, this situation is still very different from block coding, where there are $2^{n_f R_t}$ possible sequences even when n is much less than n_f.

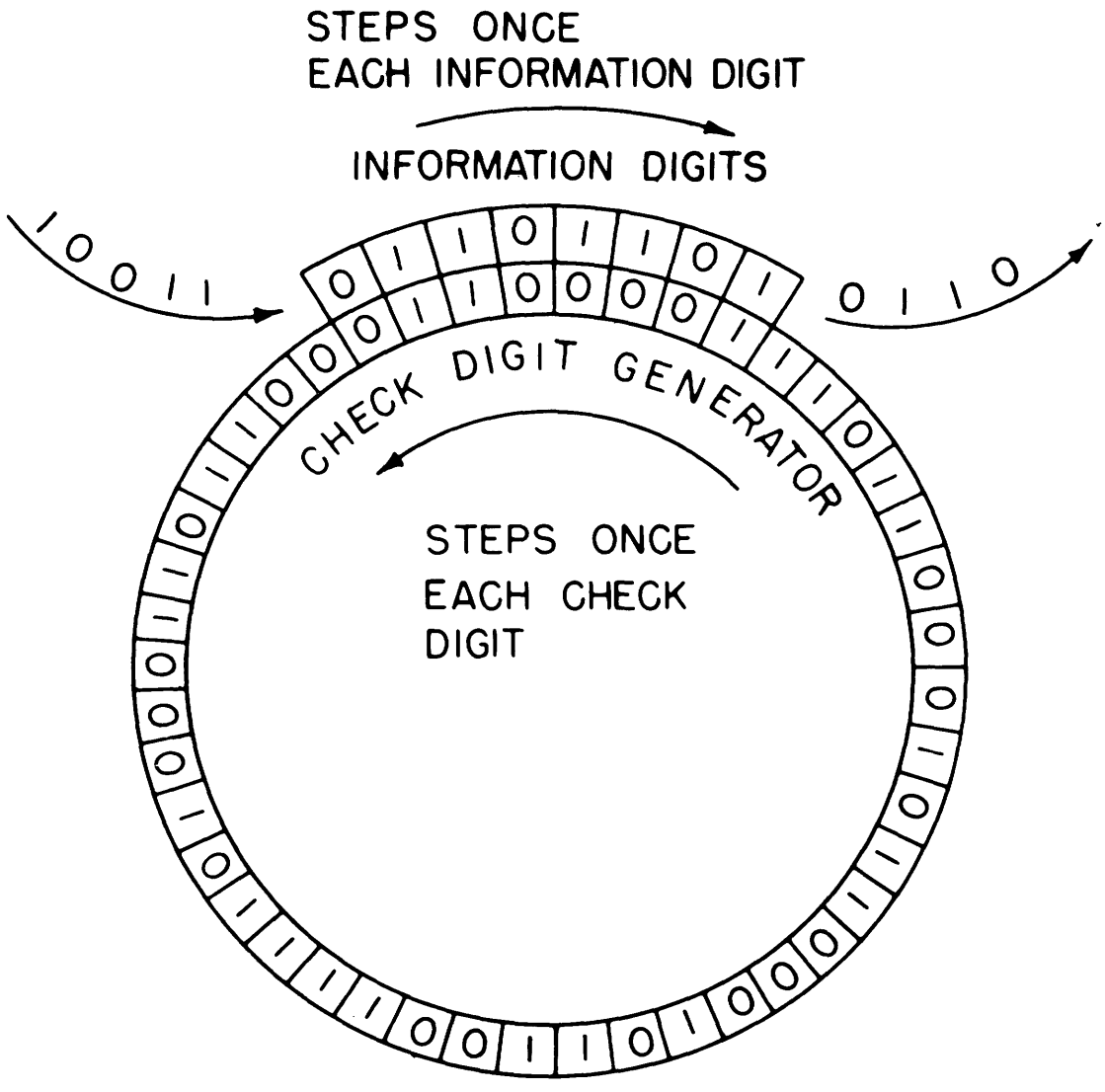

Figure 3-2

CONVOLUTIONAL MESSAGE SET GENERATION

Second, given enough time, a relatively small digital computer can generate the entire set S. This is true of any check digit code. Only a simple program and the n_f digits of the generator sequence need be stored in the computer memory.

Third, the fact that the complete code book set S forms a group, regardless of how long the sequences concerned may be, is important. It is shown in the discussion of symmetry in Chapter II that the set of distances d_i between a received message y and the members of any group code book S is invariant with respect to which particular sequence is transmitted. Since the decoding procedure which we investigate in Chapter IV depends only upon these distances, without loss of generality we may assume for purposes of analysis that the transmitted sequence s_o is always the identity element of all zeros.

The constraints imposed upon S by the generator sequence g extend over a span of n_f digits, and are periodic. As mentioned in Section 1 of this chapter, the sequential decoding procedure with which we are concerned involves distance measurements between S and the next n_f as yet undecoded digits in the received message y. Accordingly, for convolutional coding the length parameter n_f has much the same significance as in block coding — it measures the length of the statistical constraints within S.

Let us define a truncated message set S_f, to comprise all of the $2^{n_f R_t}$ possible messages of length n_f that are consistent with the already-determined part of the information sequence x_o. Since the receiver is restricted to looking no more than n_f digits ahead,

only the appropriate truncated set S_f is involved at any stage in the decoding process.

When the transmitted sequence s_o is assumed to be identically zero, and no prior errors are made, the truncated set S_f is also a group. In fact, it differs from the "embryonic" set S that is generated by the first n_f encoding operations only in regard to the initial position of the convolving wheel. In so far as evaluating the sequential decoding scheme of Chapter IV is concerned, we are interested in the behavior of S_f over the ensemble of all 2^{n_f} possible generator sequences g. Since averaging over the ensemble destroys the significance of the initial orientation of g, S_f may always be considered statistically equivalent to the embryonic set S. The general validity of an analysis on this basis is restricted only by the specific assumption that no errors have been made beforehand.

The receiver attempts in any one stage of decoding to identify only the next as yet undetermined information digit. Since the transmitted sequence s_o is assumed to be all zeros, we are especially concerned with the behavior of that subset of S_f which contains all messages s_i corresponding to possible information sequences x_i whose first digit is 1. We call this subset S_1, and recognize that it contains every sequence in S_f that is really "incorrect," at least in so far as the decoding procedure is concerned. By elimination, the "correct" subset S_o is complementary to S_1, and contains all of the possible transmitted sequences whose corresponding first information digit is a zero. This notation is indicated in Fig. 3-1.

Consider any particular sequence s_i that is a member of the incorrect subset S_1. The leading digit of the corresponding information sequence x_i is then a 1. As x_i passes through the window of the convolutional encoding device, this 1 plays against each of the n_f digits of the generator sequence g in turn. For any particular choice of g, a particular sequence s_i is generated. For any different g, s_i also is different. Accordingly, over the ensemble of all possible generators g, each s_i in S_1 is equally likely to be any binary sequence whatsoever.

The embryonic little set S illustrated in Fig. 3-1 results when $n_o = 3$, $R_t = 1/3$, and the generator sequence g is given by

$$g = 0\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 0$$

We see from the figure that this is a reasonably good choice for g, since every sequence in the incorrect subset S_1 differs from the supposedly transmitted sequence of all zeros in approximately 1/2 of its digits. Furthermore, the entire set S has a thoroughly mixed-up appearance. On account of the general random coding argument, we anticipate that both of these effects are characteristic of good code sets. In convolutional coding we may reasonably expect similar results whenever g itself contains approximately 1/2 ones, and involves as few periodicities as possible.

CHAPTER IV

SEQUENTIAL DECODING

1. The Decoding Concept

For any specific set S of possible transmitted messages, the general maximum-likelihood decoding procedure involves comparing the received message y against each of the sequences s_i in S. The receiver then decides that the sequence differing from y in the fewest digits is the transmitted message s_0, and prints the corresponding information sequence x_0.

As pointed out in Chapter II, this general maximum-likelihood procedure is impracticable when extremely small probabilities of error and a constant rate of information transmission are demanded concurrently. In our search for good decoding techniques, however, we are not necessarily limited to considering only procedures of an ideal maximum likelihood nature. Depending upon the characteristics of S, other detection criteria may exist that are sufficiently near-optimum from the point of view of error probability, and at the same time feasible from the point of view of implementation. In particular, the convolutional encoding technique discussed in the preceding chapter results in a message set that is especially amenable to a modified decoding strategy.

It is shown in Chapter III that the structure of a convolutional code book set is tree-like. This characteristic is emphasized in Fig. 4-1, where the set S itself is identical with that of Fig. 3-1, but is drawn in a slightly different form.

In encoding, the transmitter is given some information

sequence x_0. It then generates the corresponding transmitted message s_0, by convolving x_0 against the check digit generator g in accordance with the rules outlined in the preceding chapter. This procedure is exactly equivalent to tracing out a particular path through the tree-structure of S. Each successive digit of x_0 can be interpreted as an "instruction" to the transmitter, where the symbol 0 means "go up" at a node, and 1 means "go down." This convention is indicated on the figures.

We are interested in a sequential decoding technique, by which we mean that each of these "instructions" is determined in turn, one after the other. At any particular stage of the process, there is only one binary decision to be made: Did the transmitter trace next along the upper or along the lower branch of the tree? The decoder attempts to answer this question by comparing the received message y against S.

Within a transmitted sequence s_0, the influence exerted by any single encoding instruction extends over a span of n_f digits. Accordingly, we restrict the receiver to observing no more than the next n_f digits of y. At any one decoding operation, we are then concerned only with the truncated code book set S_f, defined in Chapter III to include every possible message of length n_f that is consistent with the already-determined part of the information sequence x_0.

On account of the symmetry characteristics of group codes, it is perfectly general to assume that the transmitted message s_0 is always the identity sequence of all zeros. In the absence of

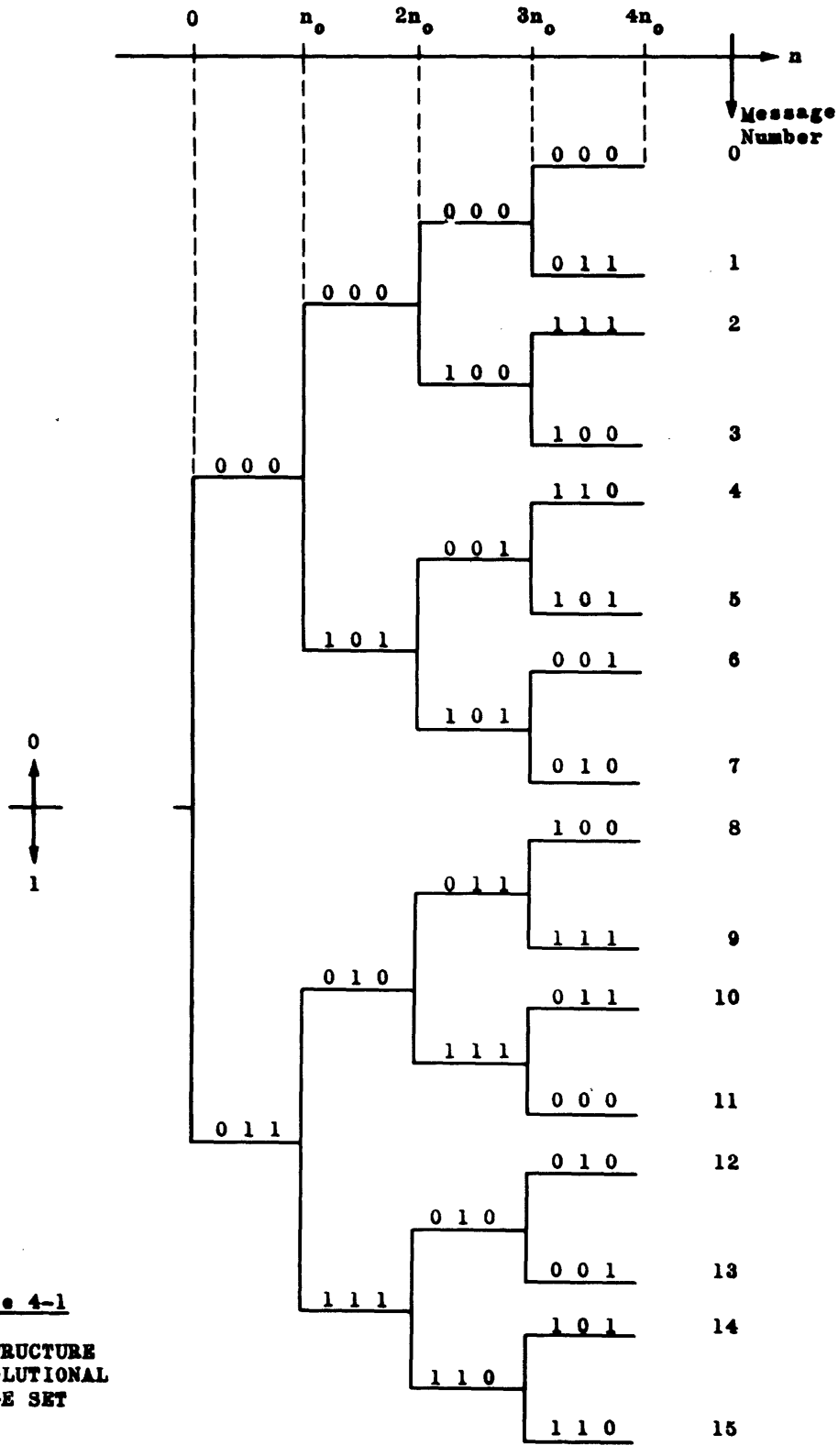

Figure 4-1

TREE-STRUCTURE OF CONVOLUTIONAL MESSAGE SET

prior decoding errors, therefore, we can consider the truncated set S_f to be statistically equivalent to the embryonic set S of all possible messages generated by the initial n_f operations of the encoding mechanism.

For this situation, in so far as the single required binary decoding decision is concerned, all of the messages in S_f that correspond to information sequences beginning with a 1 are incorrect. This subset of S_f is defined as S_1, and the complementary subset corresponding to the initial encoding instruction 0 is defined as S_0.

A sufficient maximum-likelihood detection procedure consists of showing that at least one of the sequences in the correct subset S_0 is more likely than any sequence s_i in the incorrect subset S_1 to have resulted in the received message y. Unfortunately, such a procedure is still unattractive, since S_1 itself contains exponentially-many members.

This difficulty with exponential growth can be avoided — at a reasonable cost, in terms of increased error probability — by programming a decoding computer to eliminate from further consideration any sequence that is sufficiently improbable with respect to the received message y. This is the key concept in the decoding strategy which we now propose. The word "improbable" must, of course, be precisely defined.

2. The Probability Criterion K

Let us assume, rather arbitrarily at first, that "improbable" means "less probable than 2^{-K}." The positive number K is then a probability criterion.

As pointed out in Chapter III, a digital computer can produce, if necessary, each sequence in the truncated message set S_f in turn, and compare it against the received signal y. If it is to discard those sequences that are less probable than 2^{-K}, however, then we must provide a corresponding distance criterion k, such that

$$P(d_o > k) = 2^{-K} \tag{4.1}$$

where d_o represents the number of digits out of n in which the transmitted and received sequences differ. The value of k that satisfies Eq.(4.1) is a function both of the probability criterion K and of the observed sequence length n, which can be any positive number less than or equal to n_f. In order to emphasize this implicit n-dependence, we hereafter write the distance criterion k as k_n.

Exact determination of the function k_n specified by Eq.(4.1) involves the solution for k_n of the equation

$$\sum_{j=k_n+1}^{n} p_o^j \, q_o^{n-j} \binom{n}{j} = 2^{-K} \tag{4.2}$$

where p_o is the channel transition probability, and $q_o = 1 - p_o$. Furthermore, Eq.(4.2) must be solved for every value of n from 1 to n_f. This is a quite formidable task. However, we can simplify matters conceptually by using the following inequality due to Shannon, which is derived in Appendix A.

$$P(d_o > np) \leqslant 2^{-n\left[H(p_o)-H(p)+(p-p_o)\log \frac{q_o}{p_o}\right]} \quad (\text{for } p > p_o) \tag{A.30}$$

The parameter p in Eq.(A.30) is arbitrary, except that it must exceed p_o.

Let us equate the right-hand sides of Eqs.(4.1) and (A.30), define $E_K = K/n$, and call the value of p that satisfies the resulting equation p_K.

$$E_K = \frac{K}{n} = H(p_o) - H(p_K) + (p_K - p_o)\log \frac{q_o}{p_o} \tag{4.3}$$

Then an approximate solution to Eq.(4.1) is obtained by setting

$$k_n = np_K \tag{4.4}$$

Equation (4.3) expresses an implicit transcendental relation defining p_K in terms of K and n. The form of the equation is identical with that of Eq.(A.52), and a geometric interpretation is again instructive. In Fig. 4-2, the line drawn tangent to the curve H(p) at $p = p_o$ has a slope $m = H_o' = \log \frac{q_o}{p_o}$. For any values K and n, we construct a line segment of length $E_K = K/n$, hold it vertical, and slide it to the left between H(p) and the tangent. The value of the abscissa when E_K fits precisely is p_K.

For fixed length n, it is immediately apparent from this geometric construction that p_K, and hence k_n, is a monotonically increasing function of K. Also, in accordance with the basic relations of probability theory, we know that k_n must increase approximately as the square root of n, for fixed K.

The function k_n which we obtain by solution of Eqs.(4.3) and (4.4) is actually a conservative approximation to the true function specified by Eq.(4.1). By "conservative," we mean that the values of k for which $P(d_o > k) = 2^{-K}$ are everywhere overbounded by those given by the approximate solution.

In order to preserve the mathematical rigor of certain arguments in Chapter VI concerning the probability of error, we actually require that k_n be the exact solution of Eq.(4.2). In so far as this present chapter is concerned, however, we need only consider the approximate solution. The results which we obtain in this fashion are not only always conservative, but their derivation is facilitated by reference to the geometric construction of Fig. 4-2.

Many of the purely mathematical details of the analysis that follows are provided in Appendix C, to which frequent reference is made.

3. Elimination of the Incorrect Subset

Having defined a probability criterion K, and determined the (approximate) associated distance criterion function k_n, we are in a position to ask instructive questions about the behavior of the incorrect subset S_1. Let us consider a decoding computer which starts out to generate this entire subset. As it proceeds, however, it discards every sequence s_i that becomes less probable than 2^{-K} — that is, every sequence for which the distance d_i from the received sequence y becomes greater than k_n digits out of n.

The procedure is as follows. The computer begins at n = 1, and works out along the topmost path of the tree-structure of S_1 (illustrated in Fig. 4-1). The decoder progresses along this path until, at some length n, d_i exceeds k_n. This can happen for n much less than n_f. Then the computer backtracks to the node it has just passed, and proceeds out along the next lowest unexplored branch leading from that node. The computer continues in this methodical

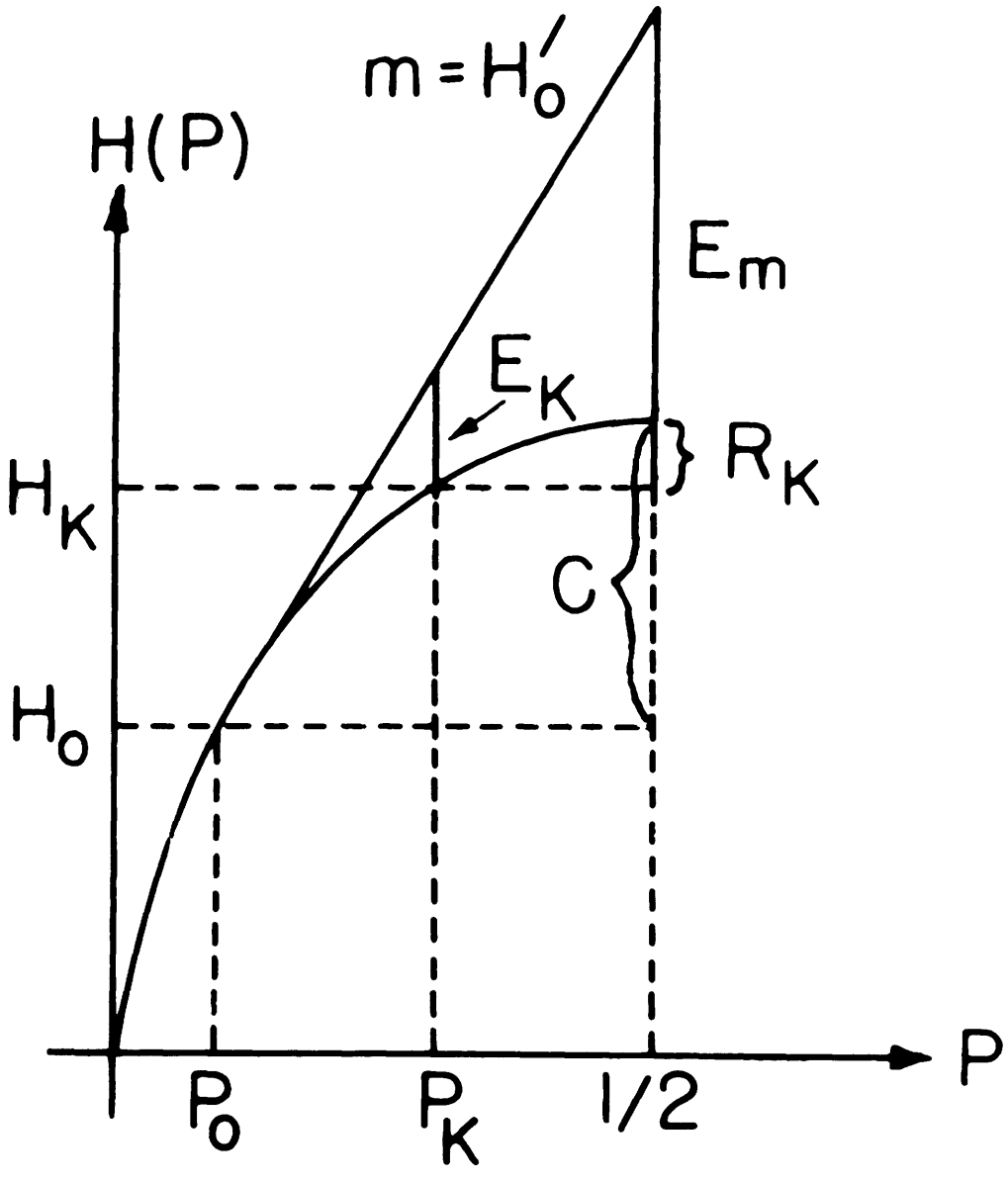

Figure 4-2

GEOMETRIC CONSTRUCTION

H_K means $H(p_K)$

H_o means $H(p_o)$

fashion, keeping always as high up in the tree as it can and still explore new branches. When all of the branches diverging from any node have been discarded, the computer backs as far as may be necessary in order to again find virgin territory.

By adopting this procedure, we minimize the storage requirements in the computer. It need keep track only of the sequence s_i with which it is currently involved. Eventually, of course, we expect the entire subset to be discarded, since S_1 contains by definition only messages that are incorrect.

The question of greatest import concerns the magnitude of "eventually." Let us define a binary computation to mean the convolutional generation of a binary digit, plus its comparison against the corresponding received digit in y. We then define $\overline{N}_K$ to be the average number of binary computations required to eliminate the entire incorrect subset S_1, subject to the probability criterion K. The averaging, as usual, is over the ensemble of all possible convolutional generator sequences g.

First of all, let us represent the number of binary computations required to extend any sequence in S from length n to length (n+ 1) by $\Delta(n)$. This may be equal to either 2 or 1, depending upon whether or not there is a node in the tree-structure at length n. In any event, $\Delta(n)$ is a perfectly definite function of n only.

Assume in a particular experiment that the number of messages of length n in S_1 that are probable according to criterion K is $M_K(n)$, and that no sequences have been discarded previously. The

number $N_K(n)$ of computations required to progress to length $(n+1)$ would then be $\Delta(n)M_K(n)$. The possibility that some messages may, in fact, already have been discarded for smaller n can only decrease this figure. Accordingly,

$$N_K(n) \leqslant \Delta(n)M_K(n) \tag{4.5}$$

The total number of binary computations N_K can be bounded by summing $N_K(n)$ over n, from 1 to n_f.

$$N_K \leqslant \sum_{n=1}^{n_f} \Delta(n)M_K(n) \tag{4.6}$$

Finally, since the average of a sum equals the sum of the averages, over the ensemble of generator sequences we have

$$\overline{N}_K \leqslant \sum_{n=1}^{n_f} \Delta(n)\overline{M}_K(n) \tag{4.7}$$

In order to evaluate Eq.(4.7), we make use of one of the results proved in Chapter III. It is shown there that, as the convolutional generator g assumes all possible values, any particular message s_i in the incorrect subset S_1 runs in one-to-one correspondence through the set of all 2^{n_f} binary numbers of length n_f. This is true of each and every sequence s_i. Accordingly, over the ensemble of all g's, any s_i is statistically independent of the received message y.

In Appendix A, we also derive another result due to Shannon, which applies to the distance between two statistically independent binary sequences.

$$P(d_i \leqslant np) \leqslant 2^{-n\left[1-H(p)\right]} \qquad (\text{for } p < \tfrac{1}{2}) \tag{A.32}$$

Specifically, let d_i represent the distance between the sequences s_i and y, and set the arbitrary parameter p equal to p_K. We then have

$$P(d_i \leqslant k_n) \leqslant 2^{-nR_K(n)} \qquad (\text{for } k_n < \tfrac{1}{2} n) \tag{4.8}$$

where k_n is the distance criterion function associated with the probability K, and $R_K(n)$ is defined by

$$R_K(n) = 1 - H(p_K) \qquad (\text{for } p_K < \tfrac{1}{2}) \tag{4.9}$$

Equation (A.32) is rigorously correct for any $p < \frac{1}{2}$. Use therein of the approximate parameter p_K, derived from Eqs.(4.3) and (4.4), results in an approximation to $P(d_i \leqslant k_n)$ which overbounds its true value for the k_n that actually satisfies Eq.(4.2).

The geometric construction of $R_K(n)$ is illustrated in Fig. 4-2. For fixed K, $R_K(n)$ is asymptotic to the channel capacity C, as n approaches infinity and $E_K = \frac{K}{n}$ approaches zero. For small n, on the other hand, the maximum permissible value of p_K for which Eq. (4.8) is valid is 1/2, which implies that E_K equals the value E_m shown in the figure. Accordingly, for a given K, we extend the definition of Eq.(4.9) to set

$$R_K(n) = 0 \qquad (\text{for } n \leqslant (n_K)_{min} = \tfrac{K}{E_m}) \tag{4.10}$$

This means, essentially, that more than $(n_K)_{min}$ digits must be compared before it is possible to assert with probability $\left(1 - 2^{-K}\right)$ that any sequence s_i is not the transmitted sequence s_o.

It is evident from the geometric construction that $R_K(n)$ is a monotonically increasing function of n, and a monotonically decreasing function of K. A sketch of $R_K(n)$ is included as Fig. 4-3; its dimensions are those of a rate of transmission.

Since Eq.(4.8) holds for each sequence s_i in the subset S_1, over the ensemble of all possible check digit generator sequences g the average number of incorrect sequences of length n that are probable according to criterion K is bounded by

$$\bar{M}_K(n) \leqslant \left|S_1(n)\right| \; 2^{-nR_K(n)} \tag{4.11}$$

where $\left|S_1(n)\right|$ is the total number of sequences of length n in S_1. Equation (4.10) again follows from the fact that the average of a sum is equal to the sum of the averages. Substituting Eq.(4.11) into Eq.(4.7), we obtain the inequality

$$\bar{N}_K \leqslant \sum_{n=1}^{n_f} \Delta(n) \left|S_1(n)\right| \; 2^{-nR_K(n)} \tag{4.12}$$

It is mentioned in Chapter III that the number of sequences in the complete tree set S is approximately equal to 2^{nR_t}, where n is the length of the set and R_t is the rate of transmission of information. When account is taken of the fact that the tree-structure of S_1 branches only at a discrete set of nodes, we can write the rigorous inequality

$$\left|S_1(n)\right| \leqslant D_o \; 2^{nR_t} \tag{C.5}$$

where

$$D_o = \tfrac{1}{2} \, 2^{(n_o-1)R_t} \tag{C.6}$$

In Eq.(C.6), n_o is the branch length. This result is derived in Appendix C. In Section 3 of that appendix, we also obtain the bound

$$\Delta(n)\left|S_1(n)\right| \leqslant D_o \; 2^{(n+1)R_t} \tag{C.40}$$

Substituting Eq.(C.40) into Eq.(4.12) strengthens the inequality.

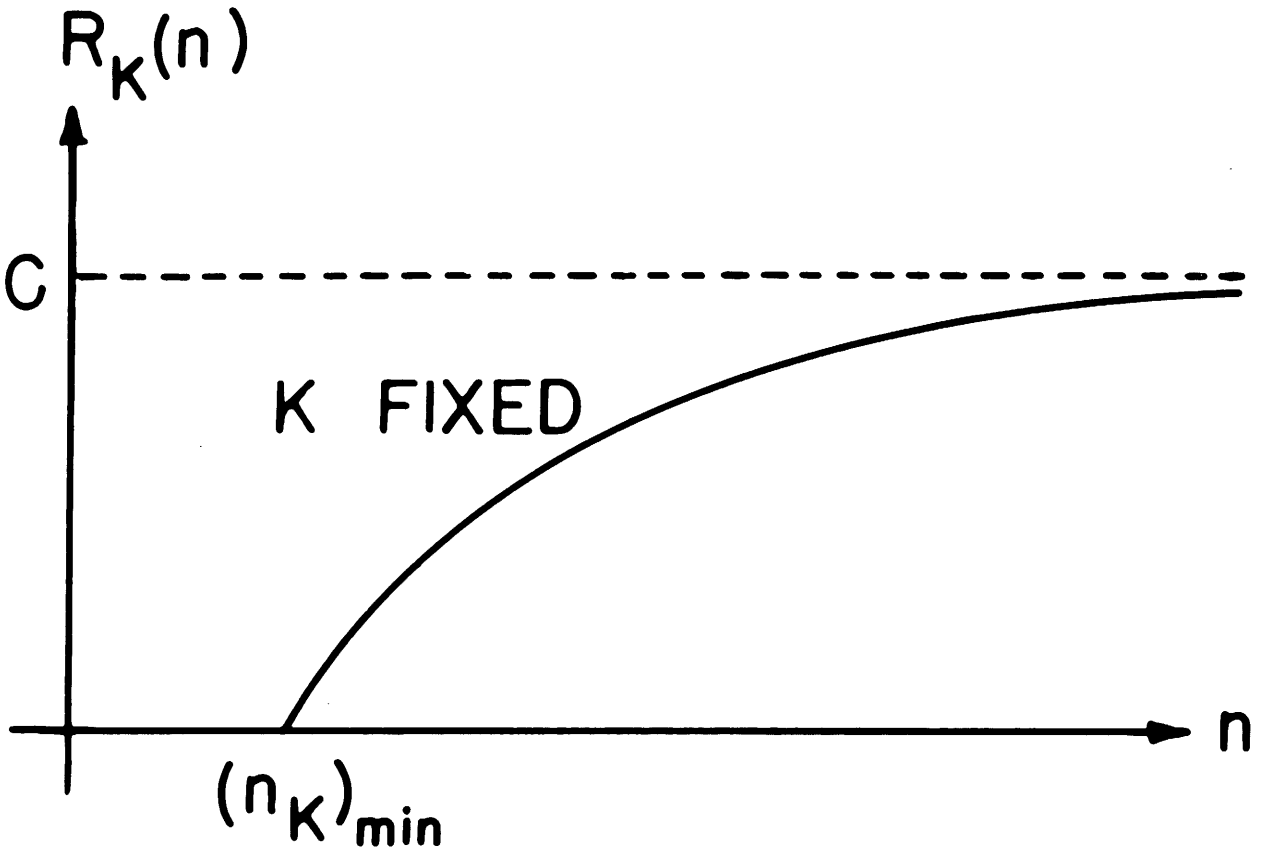

Figure 4-3

SKETCH OF THE FUNCTION $R_K(n)$

Finally, therefore,

$$\bar{N}_K < D_1 \sum_{n=1}^{n_f} 2^{n\left[R_t - R_K(n)\right]} \tag{4.13}$$

where

$$D_1 = 2^{(n_o R_t - 1)} \tag{4.14}$$

We may also substitute Equation (C.5) into Eq.(4.11), and obtain the result

$$\bar{M}_K(n) \leqslant D_o \, 2^{n\left[R_t - R_K(n)\right]} \tag{4.15}$$

In terms of $\bar{M}_K(n)$, Eq.(4.13) becomes

$$\bar{N}_K < 2^{R_t} \sum_{n=1}^{n_f} \bar{M}_K(n) \tag{4.16}$$

Algebraic Bound to $R_K(n)$. Equation (4.13) is the desired bound on the ensemble average number of binary computations $\bar{N}_K$ required to eliminate the entire subset S_1 of incorrect messages as "improbable according to criterion K." Unfortunately, direct evaluation of the r.h.s. of Eq.(4.13) requires numerical methods, since the function $R_K(n)$ is defined by Eq.(4.9) in terms of the implicit transcendental parameter p_K, which in turn is determined approximately as the solution to Eq.(4.3).

In spite of this difficulty, an idea of the general nature of $\bar{N}_K$ results from consideration of $\bar{M}_K(n)$. Since $R_K(n)$ is identically zero for $n < (n_K)_{min} = \frac{K}{E_m}$, $\bar{M}_K(n)$ grows exponentially as 2^{nR_t} for small values of n. For larger values of n, $R_K(n)$ increases monotonically towards its asymptotic value C. When the rate of transmission R_t is less than C, therefore, $R_K(n)$ crosses R_t at

some value of n. Thereafter, the exponent in Eq.(4.15) is negative, and $\overline{M}_K(n)$ becomes negligibly small.

A typical sketch of the function $\overline{M}_K(n)$ is provided in Fig. 4-4. Since $R_K(n)$ is monotone increasing, $\overline{M}_K(n)$ has a single maximum term. Accordingly, we are guaranteed that the summation bounding $\overline{N}_K$ in Eq.(4.16) is well behaved. Furthermore, for a given value of the probability criterion K, we do not expect the summation $\overline{N}_K$ to be a sensitive function of the length parameter n_f. All of these results, of course, are directly attributable to the fact that the total number of possible transmitted sequences in the convolutional set S varies only as 2^{nR_t}, instead of being equal to $2^{n_f R_t}$ for all n as in block coding.

Difficulty in the evaluation of the bound on $\overline{N}_K$ is avoided when an appropriate algebraic function of K and n is used in place of $R_K(n)$ in Eq.(4.13). In Appendix B, we show that $R_K(n)$ is always such that

$$R_K(n) \geqslant C - \frac{2C}{\sqrt{E_m}}\sqrt{\frac{K}{n}} + \frac{C}{E_m} \cdot \frac{K}{n} \qquad \text{(B.28)}$$

$$(\text{for } n > (n_K)_{min})$$

In this equation, C is the channel capacity, and E_m is the maximum permissible value of $E_K = \frac{K}{n}$, as illustrated in Fig. 4-2.

$$E_m = \left(\frac{1}{2} - p_o\right) \log \frac{q_o}{p_o} - C \qquad \text{(B.5)}$$

Upper Bound to $\overline{N}_K$. Substitution of this algebraic bound on $R_K(n)$, over the range $(n_K)_{min} < n \leqslant n_f$, into the bound on $\overline{N}_K$ given by Eq.(4.13) again strengthens the inequality. For smaller values

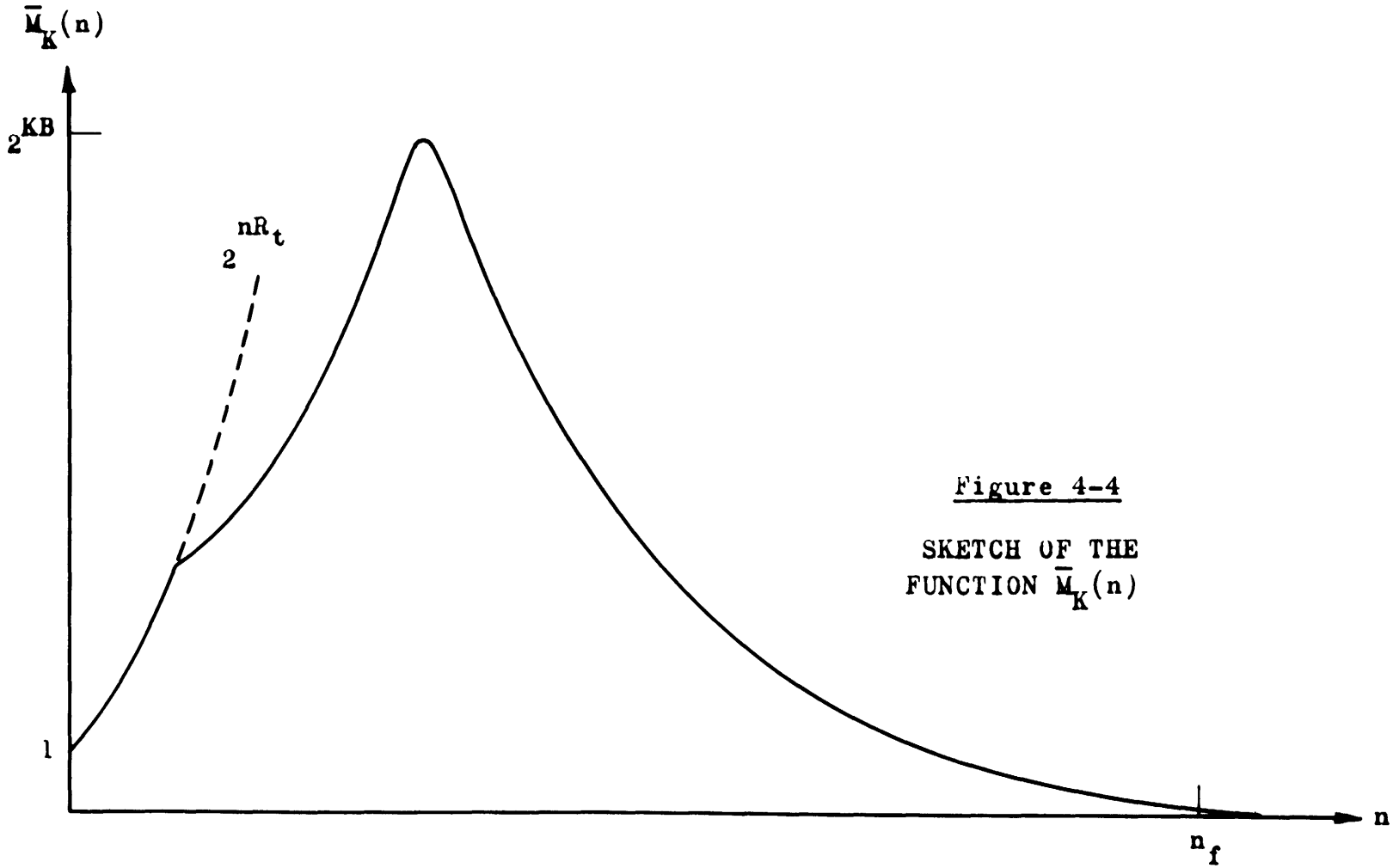

Figure 4-4

SKETCH OF THE FUNCTION $\bar{M}_K(n)$

of n, $R_K(n)$ is still defined in accordance with Eq.(4.10) to be identically zero. As a consequence, every sequence in S_1 must be generated for $n \leqslant (n_K)_{min} = K/E_m$. From Eq.(C.5) there are no more than $D_o 2^{(n_K)_{min}R_t}$ such sequences in total at the upper limit of this restricted range of n ; also, as is evident from Fig. 4-1, this number decreases as $2^{-n_o R_t}$ each time n decreases towards zero by an amount n_o. Accordingly, we can rewrite Eq.(4.13) in the form

$$\bar{N}_K < \frac{n_o D_o}{1 - 2^{-n_o R_t}} 2^{(n_K)_{min}R_t} + D_1 \sum_{n=(n_K)_{min}}^{n_f} 2^{n\left[R_t - C + \frac{2C}{\sqrt{E_m}}\sqrt{\frac{K}{n}} - \frac{C}{E_m}\frac{K}{n}\right]} \qquad (4.17)$$

The maximum term in the summation above is equal to 2^{KB}, where the extremely important parameter B is defined by

$$B = \frac{CR_t/E_m}{C - R_t} \qquad (4.18)$$

Finally, since a finite sum is bounded by the number of terms times the maximum term, we have the rough bound that

$$\bar{N}_K < D_1 \, n_f \, 2^{KB} \qquad (4.19)$$

It is also possible to obtain a much tighter evaluation of the r.h.s. of Eq.(4.19). When the summand has a single maximum, a summation over unit steps is bounded above by the corresponding integral plus the maximum term. This calculation is carried out in detail in Appendix C, with the result that the factor n_f in the rough bound of Eq.(4.19) is eliminated.

$$\bar{N}_K \leq D_1 \left[(D_2 + D_3)\, 2^{K \frac{R_t}{E_m}} + (1 + D_4 \sqrt{K})\, 2^{KB} \right] \qquad (C.18)$$

where

$$D_1 = 2^{(n_o R_t - 1)} \qquad (4.14)$$

$$D_2 = \frac{n_o\, 2^{-R_t}}{1 - 2^{-n_o R_t}} \qquad (C.19)$$

$$D_3 = \frac{\log e}{C - R_t} \qquad (C.20)$$

$$D_4 = \frac{2C}{(C - R_t)^{3/2}} \sqrt{\frac{\pi \log e}{E_m}} \qquad (C.21)$$

These inequalities bound the average number of binary computations that a decoding computer must perform in order to eliminate the entire incorrect subset S_1 in accordance with the probability criterion K. The averaging is over the ensemble of all 2^{n_f} possible convolutional generator sequences g.

Although we cannot be certain about the behavior in this respect of a convolutional message set S generated by any particular sequence g, as usual we are certain that most such sets are substantially as good as the ensemble average of all sets. This follows again, as in the discussion of error probabilities in Chapter II, from Shannon's argument that when the average value of a set of positive quantities is P, no more than $\frac{1}{\rho}$ of them can exceed ρ P.

4. The Decoding Procedure

The decoding objective of the receiver is to determine, on the basis of the received sequence y, which of the two subsets of

all possible messages is S_o and which is S_1. By definition, the correct subset S_o contains the transmitted message s_o, and S_1 does not.

In the preceding section, an operational procedure is specified whereby a digital computer could, if desired, search progressively through the complete truncated message set S_f, where S_f is defined to comprise both S_o and S_1. The method is to establish a probability criterion K, and to eliminate from further consideration any sequence that becomes less probable than 2^{-K} with respect to y. With this procedure, we expect the entire incorrect subset S_1 to be discarded; the ensemble average number of binary computations required to accomplish this result is bounded by the expressions of Eq. (4.19) or (C.18). The fact that these bounds on $\overline{N}_K$ are insensitive functions of the observation span n_f encourages the incorporation of this kind of search procedure into a set of decoding rules.

Let us consider next how the prescribed search procedure reacts upon the correct subset S_o, which includes the transmitted sequence s_o. The distance criterion function k_n is defined by Eq. (4.1) to be such that

$$P(d_o > k_n) = 2^{-K} \tag{4.1}$$

where d_o represents the number of digits out of n in which the received message y differs from s_o. This inequality is valid for every value of n, from 1 to n_f. Since, in searching through S_o, the computer has a total of n_f opportunities to discard s_o,

$$P(s_o \text{ discarded}) \leqslant n_f\, 2^{-K} \tag{4.20}$$

Equation (4.20) follows directly from the fact that the probability of a union of events can be no greater than the sum of the probabilities of its constituents. Finally, since the entire correct subset S_0 can be eliminated only if the transmitted sequence s_0 is discarded, we have the result

$$P(S_0 \text{ discarded}) \leqslant n_f \, 2^{-K} \qquad (4.21)$$

It is interesting to consider a computer that searches through the truncated set S_f in accordance with a criterion K, and finds that one of the two (as yet unidentified) subsets is eliminated completely. Equation (4.21) means that the computer can then assert that the remaining subset is S_0. Furthermore, it can do so without ever actually finding any "probable" message. The ensemble average probability that the assertion is wrong is less than $n_f 2^{-K}$, and is independent of the channel error pattern. If the computer is programmed to operate more or less alternately upon each of the two subsets until one of them is discarded, then the ensemble average of the total number of computations is bounded by $2n_f 2^{KB}$.

For a single criterion K, the bound on the required number of computations is an increasing, and the bound on the probability of error a decreasing, exponential function of the criterion K. However, these exponents differ not only in sign but also by the factor B.

The Decoding Rules. We can specify a decoding procedure that exploits the existence of this extra factor B in the exponent of the bound on $\overline{N}_K$. Instead of a single probability criterion K, we require an increasing sequence of criteria K_1, K_2, K_3, ... , where we arbitrarily require that

$$K_j = K_1 + (j-1)\,\Delta K \qquad (4.22)$$

With this definition of K_j, let us consider a decoding computer that searches through the truncated message set S_f in accordance with the following rules.

(a) The computer begins with the smallest criterion K_1, and starts out to generate sequentially the entire truncated set S_f. As the computer proceeds, it discards any sequence that differs from the received message in more than k_n digits out of n.

(b) As soon as the computer discovers any sequence in S_f that is retained through length $n = n_f$, it prints the corresponding first information digit.

(c) If the complete set S_f is discarded, the computer adopts the next larger criterion (K_2), and starts over again from the beginning. It continues this procedure until <u>some</u> sequence in S_f <u>is</u> retained through length $n = n_f$. It then prints the corresponding first information digit.

(d) The decoder repeats the above procedure in its entirety for each successive information digit in turn.

When these rules are adopted, the computer never uses a criterion K_j unless the correct subset S_o (and hence the transmitted sequence s_o) is discarded for K_{j-1}. The probability that s_o is discarded depends, of course, only upon the channel noise pattern Ψ_o, and is statistically independent of the ensemble of possible convolutional generator sequences g. Accordingly, we may determine a number $\overline{N}$, which we define to be the average total number of binary computations required to eliminate the incorrect subset S_1. We do

this by averaging $\bar{N}_K$ with respect to the probability that the j^{th} criterion K_j is used.

Let $\bar{N}_j$ represent the value of $\bar{N}_K$ when $K = K_j$, and let $P(j)$ be the probability that the decoder uses the j^{th} criterion. Then

$$\bar{N} = \sum_j P(j)\bar{N}_j \tag{4.23}$$

Since the j^{th} criterion is reached only when S_o is discarded for K_{j-1}, we have from Eq.(4.21) the bound

$$\begin{aligned} P(j) &\leqslant n_f\, 2^{-K_{j-1}} && (\text{for } j \geqslant 2) \\ &= 1 && (\text{for } j = 1) \end{aligned} \tag{4.24}$$

When Eqs.(4.19), (4.22), and (4.24) are substituted into Eq.(4.23), we obtain a bound on $\bar{N}$. This bound, of course, involves the arbitrary parameters K_1 and ΔK that are used in the definition of K_j. In Appendix C, the computation is carried out in detail, and it is shown that the values of K_1 and ΔK which minimize a rough bound on $\bar{N}$ are given by

$$\Delta K = \frac{\log B}{B - 1} \tag{C.30}$$

and

$$K_1 = \log \frac{n_f}{B^{1/1-B}} \tag{C.31}$$

The final result, which is valid only for values of B less than unity, is shown to be

$$\bar{N} < n_f^{(1+B)} \cdot \frac{D_1}{1 - B} \cdot \left(\frac{1}{B}\right)^{B/1-B} \quad (\text{for } B<1) \tag{C.32}$$

Equation (C.32) is derived through use of the rough overbound on $\bar{N}_K$ given by Eq.(4.19). It is also possible to use the much

tighter bound of Eq.(C.18). This calculation is shown in Appendix C to lead to the result

$$\bar{N} < D_1 \left[(D_2 + D_3)\, 2^{K_1 \frac{R_t}{E_m}} + (1 + D_4\sqrt{K_1})\, 2^{K_1 B} \right]$$

$$+ n_f D_1 \left\{ (D_2 + D_3)\, 2^{-K_1\left(1 - \frac{R_t}{E_m}\right)} \left(\frac{2^{\Delta K \frac{R_t}{E_m}}}{1 - 2^{-\Delta K\left(1 - \frac{R_t}{E_m}\right)}} \right) \right.$$

$$\left. + 2^{-K_1(1-B)} \left(\frac{2^{\Delta K}}{1 - 2^{-\Delta K(1-B)}} \right) \left[1 + \frac{D_4}{\sqrt{K_1 + \Delta K}} \left(K_1 + \frac{\Delta K}{1 - 2^{-\Delta K(1-B)}} \right) \right] \right\}$$

(for $B < 1$) (C.34)

Minimization of Eq.(C.34) with respect to K_1 and ΔK requires numerical trial-and-error methods. However, to a good approximation, the values given in Eqs.(C.30) and (C.31) are still substantially optimum. It is shown in Appendix C that their substitution into Eq.(C.34) leads to a bound on $\bar{N}$ that increases with n_f no faster than $n_f^B \sqrt{\log D_6 n_f}$, where D_6 is some constant independent of n_f.

These bounds on $\bar{N}$, the ensemble average of computations required to eliminate the incorrect subset S_1, are valid only for $B<1$, where B is defined as

$$B = \frac{CR_t/E_m}{C - R_t} \tag{4.18}$$

The equivalent constraint on the rate of transmission is

$$R_t < \frac{C}{1 + C/E_m} \tag{4.25}$$

For higher rates of transmission, the bound on $\overline{N}_j$ increases faster than $P(j)$ decreases, and the computation for $\overline{N}$ does not converge. From a practical point of view, since from Eq.(C.32) the bound on $\overline{N}$ increases as $\frac{1}{1-B} \cdot \left(\frac{1}{B}\right)^{B/1-B}$, this is no great disadvantage. We do not expect the decoding procedure to be useful for values of R_t much greater than $\frac{1}{2} C$ anyway.

Discussion. Consideration of the behavior of the bound on $\overline{N}$ with respect to the various parameters determining it, together with numerical results, is deferred until Chapter VII. The most important result is that the average number of computations which the decoder performs upon the incorrect subset S_1 is a very slowly varying function of n_f. This is a far more tractable behavior than the exponential growth that is characteristic of the general maximum-likelihood decoding procedure. Furthermore, in Chapter V we show that the resulting decoding probability of error is not much degraded.

No mention has yet been made of the number of decoding computations that are performed upon the correct subset S_0. All that is required is that the computer discover some one sequence in S_0 that is consistent with the received message y. Any such sequence will do, since a decoding decision is made only as to the first digit of the information sequence. However, it is possible that particular channel error patterns could still cause difficulties — that is, that the computer could search extensively through S_0 in accordance with a (small) criterion K_j, and succeed neither in determining a probable message nor in discarding the subset completely. This problem is discussed in detail in Chapter VI.

CHAPTER V

PROBABILITY OF ERROR

1. The Incidence of Errors

The sequential decoding scheme with which we are concerned is developed in Chapter IV from the computational viewpoint. We desire, of course, not only that the decoding procedure be capable of implementation with reasonable equipment, but also that it result in a probability of error as small as may be required. In particular, we hope for a probability-of-error behavior that is at least exponentially optimum.

Before undertaking analysis of this aspect of the problem, for convenience of reference we briefly restate the decoding rules that have been adopted. As in Chapter IV, we define the truncated message set S_f to comprise all possible transmitted sequences, n_f digits in length, that are consistent with that portion of the information sequence x_0 which has already been decoded. Furthermore, we assume that no erroneous decisions have yet been made, and that the transmitted message s_0 is the identity sequence of all zeros.

In Chapter IV, an approximation to the distance criterion function k_n, associated with the probability criterion K, is determined as the solution to Eqs.(4.3) and (4.4). This simplification assures us that the distance d_0 between the transmitted and received messages satisfies the inequality

$$P(d_0 > k_n) \leqslant 2^{-K} \tag{5.1}$$

for all n from 1 to n_f. In so far as determination of bounds on

the ensemble average number of binary computations required to eliminate the subset S_1 of incorrect messages is concerned, use of this approximation to k_n leads to conservative results.

In the present instance, however, we are concerned with bounding the probability of error, and the approximation is no longer conservative. Accordingly, we now consider the true function k_n, defined in Chapter IV to be such that

$$P(d_o > k_n) = 2^{-K} \qquad \text{(for all n)} \qquad (4.1)$$

With this understanding, the decoding rules are as follows.

(a) The receiving digital computer searches progressively through the truncated set S_f, in accordance with the smallest unused probability criterion K_j. Any sequence in S_f that becomes less probable than 2^{-K_j} is discarded.

(b) As soon as any probable sequence of length n_f is discovered, the corresponding first information digit is printed.

(c) If the entire message set S_f is discarded, the computer starts over from the beginning, using the next larger criterion K_{j+1}.

The essential feature in these rules is that a final decision to print is made only after some sequence s in S_f is found to be consistent with the received message y over the complete span n_f of the convolutional constraints imposed by the encoding mechanism. Interim decisions to discard messages as inconsistent with y are, of course, made at smaller lengths, and the transmitted sequence s_o may accordingly be rejected. However, such an event does not in itself constitute a decoding error. A printing error can occur,

for any given probability criterion K_j, if and only if one or more messages s_i in the incorrect subset S_1 is retained throughout the entire search procedure.

Let us assume that a particular selection of a convolutional generator sequence is made, and that s_o is the transmitted message. The channel perturbs s_o by adding to it, modulo-2, a noise sequence Ψ_o. In any given experiment, there exists some <u>smallest</u> criterion K_j for which the decoding computer retains any member of the correct subset S_o all the way out to length n_f.

Consider this particular criterion K_j. Every sequence in S_f that differs from the received message y in more than $(k_n)_j$ digits out of n is discarded. A necessary condition for a decoding error, therefore, is that some one s_i in S_1 shall differ from y over the total length n_f in no more than $(k_{n_f})_j$ digits. Specifically, $(k_{n_f})_j$ is the value at $n = n_f$ of the distance criterion k_n that is associated with the particular criterion K_j. Accordingly, the conditional probability of error, given that K_j is the <u>smallest</u> criterion K for which any member of the subset S_o of correct messages is retained to length n_f, is bounded by

$$P_j(e) \leqslant P_j(\text{any } d_i \leqslant k_{n_f}) \qquad (5.2)$$

In this equation, d_i represents the distance between the received message y and the i^{th} sequence in the incorrect subset S_1.

2. <u>The Average Value of $P_j(e)$</u>

Just as in the case of block coding, it is possible to bound the average value of $P_j(e)$. Since we are dealing here with a convolutional message set, this averaging is performed over the ensemble

of all possible check digit generator sequences g.

It is shown in Chapter III that, as g assumes all possible values, any sequence s_i in the incorrect subset S_1 runs in one-to-one correspondence through the set of all binary numbers of length n_f. Regardless of the specific value of the received sequence y, therefore, over the ensemble of g's the probability distribution of the distance d_i between y and any particular s_i is the same as if these two sequences were selected independently and at random with respect to each other. Accordingly, we may use the bound given by Eq.(A.32), and write in terms of the entropy function

$$P_j(d_i \leqslant k_{n_f}) \leqslant 2^{-n_f\left[1-H\left(\frac{k_{n_f}}{n_f}\right)_j\right]} \tag{5.3}$$

where the sub-j notation is used to indicate that the probability criterion K equals K_j. It is also possible to use the appropriate binomial distribution result directly, and to write the equality

$$P_j(d_i \leqslant k_{n_f}) = 2^{-n_f} \sum_{\ell=0}^{(k_{n_f})_j} \binom{n_f}{\ell} \tag{5.4}$$

The total length n_f is constrained by the convolutional encoding mechanism described in Chapter IV to be equal to an integral number of the branch lengths n_o. It follows that the number of sequences of length n_f in the incorrect subset S_1 is exactly equal to

$$\left|S_1(n_f)\right| = \frac{1}{2} 2^{n_f R_t} \tag{5.5}$$

where R_t is the rate of transmission. As in Chapter II, we may define an auxiliary parameter p_t, such that

$$R_t = 1 - H(p_t) \tag{5.6}$$

Next, we again invoke the fact that the probability of a union is bounded by the sum of the probabilities of its constituents. Therefore,

$$P_j(\text{any } d_i \leqslant k_{n_f}) \leqslant \left|S_1(n_f)\right| P_j(d_i \leqslant k_{n_f}) \tag{5.7}$$

Substituting Eqs.(5.3), (5.5), and (5.6) into Eq.(5.7), we have

$$\left.\begin{aligned} P_j(\text{any } d_i \leqslant k_{n_f}) &\leqslant \tfrac{1}{2}\, 2^{-n_f\left[H(p_t)-H\left(\frac{k_{n_f}}{n_f}\right)_j\right]} \\ &\qquad\qquad \text{(for the r.h.s.} < 1) \\ &\leqslant 1 \qquad\qquad \text{(otherwise)} \end{aligned}\right\} \tag{5.8}$$

In this equation, we are guaranteed that the top inequality applies whenever

$$(k_{n_f})_j \leqslant n_f p_t \tag{5.9}$$

Accordingly, combining Eqs.(5.4) and (5.7), we obtain the following expression for $P_j(e)$.

$$\left.\begin{aligned} P_j(e) &\leqslant \left|S_1(n_f)\right| 2^{-n_f} \sum_{\ell=0}^{(k_{n_f})_j} \binom{n_f}{\ell} \\ &\qquad\qquad \text{(for } (k_{n_f})_j \leqslant n_f p_t) \\ &\leqslant 1 \qquad \text{(otherwise)} \end{aligned}\right\} \tag{5.10}$$

3. The Average Probability of Error

Let the over-all ensemble average probability of error be denoted by $P(e_1)$. Then $P(e_1)$ is the average value of the conditional probabilities $P_j(e)$, with respect to the probability that K_j is the smallest criterion that would terminate the decoding

procedure in the absence of an error.

$$P(e_1) = \sum_j Q(j)\, P_j(e) \tag{5.11}$$

where $Q(j)$ is the probability that K_j is the smallest criterion K for which any member of the correct subset S_o is retained to length n_f.

In essence, we determine $P_j(e)$ by means of averaging over the ensemble of all of the possible convolutional codes; in Eq.(5.11), we next average over the possible channel noise patterns. This procedure is exactly the same as that used in Chapter II and Appendix A to bound the ensemble average probability of error for block codes, $P(e)_{random}$.

The decoding process terminates at least as soon as the transmitted sequence s_o itself is retained to length n_f. Accordingly, a necessary condition for K_j to be the smallest criterion for which any sequence in S_o is retained is that s_o be discarded for criterion K_{j-1}. Therefore,

$$Q(j) \leqslant P_{j-1}\ (s_o \text{ discarded}) \tag{5.12}$$

Equation (4.1) specifies the distance criteria $(k_n)_j$ to be such that

$$P_{j-1}(d_o > k_n) = 2^{-K_{j-1}} \tag{5.13}$$

where d_o is the distance between s_o and the received sequence y. This equation holds true for all lengths n, from 1 to n_f. Since there are n_f chances altogether to discard s_o,

$$P_{j-1}\ (s_o \text{ discarded}) \leqslant n_f\, 2^{-K_{j-1}} \tag{5.14}$$

where we once more bound the probability of a union of events by the sum of their individual probabilities. Accordingly, $Q(j)$ is bounded by

$$\left.\begin{aligned} Q(j) &\leqslant n_f\, 2^{-K_{j-1}} && (\text{for } j \geqslant 2) \\ &= 1 && (\text{for } j = 1) \end{aligned}\right\} \qquad (5.15)$$

The criteria K_j are defined in Chapter IV by the relation

$$K_j = K_1 + (j-1)\,\Delta K \qquad (4.22)$$

Substituting into Eq.(5.7), we have

$$\left.\begin{aligned} Q(j) &\leqslant n_f\, 2^{\Delta K}\, 2^{-K_j} && (\text{for } j \geqslant 2) \\ &= 1 && (\text{for } j = 1) \end{aligned}\right\} \qquad (5.16)$$

Finally, since Eq.(4.1) holds for every value of n, we may identify 2^{-K_j} with the probability that s_o differs from y in more than $(k_{n_f})_j$ digits over the total length n_f. Then

$$\left.\begin{aligned} Q(j) &\leqslant n_f\, 2^{\Delta K}\, P_j(d_o > k_{n_f}) && (\text{for } j \geqslant 2) \\ &= 1 && (\text{for } j = 1) \end{aligned}\right\} \qquad (5.17)$$

Substitution of Eqs.(5.17) and (5.2) into Eq.(5.11) gives an expression for the average probability of error $P(e_1)$, over the ensemble of all possible convolutional generator sequences.

$$P(e_1) \leqslant P_1\,(\text{any } d_i \leqslant k_{n_f}) \qquad (5.18)$$

$$+\, n_f\, 2^{\Delta K} \sum_{j=2} P_j(d_o > k_{n_f})\, P_j\,(\text{any } d_i \leqslant k_{n_f})$$

We desire to evaluate Eq.(5.18) for those values of K_1 and ΔK that minimize the upper bound on the average number of binary computations performed by the decoding computer upon the subset S_1

of incorrect messages. These values are given in Appendix C as

$$\Delta K = \frac{\log B}{B - 1} \tag{C.30}$$

and

$$K_1 = \log \frac{n_f}{B^{1/1-B}} \tag{C.31}$$

where B is equal to

$$B = \frac{CR_t/E_m}{C - R_t} \tag{4.18}$$

The parameters ΔK, K_1, and n_f then satisfy the equation

$$n_f \, 2^{\Delta K} \, 2^{-K_1} = 1 \tag{5.19}$$

Finally, recognizing from Eq.(4.1) that $2^{-K_1} = P_1(d_o > k_{n_f})$, we may rewrite Eq.(5.18) as

$$P(e_1) \leqslant n_f \left(\frac{1}{B}\right)^{\frac{1}{1-B}} \sum_{j=1} P_j(d_o > k_{n_f}) P_j \quad (\text{any } d_i \leqslant k_{n_f}) \tag{5.20}$$

Evaluation of $P(e_1)$. In order to determine the exact values of the distance criteria $(k_{n_f})_j$, we have the difficult task of solving Eq.(4.1). Without ever doing so, however, we can still bound the r.h.s. of Eq.(5.20) by summing over every possible value that the numbers $(k_{n_f})_j$ could assume. On account of the value of K_1 given by Eq.(C.31), the initial distance $(k_{n_f})_1$ must be greater than np_o. Accordingly,

$$P(e_1) < n_f \left(\frac{1}{B}\right)^{\frac{1}{1-B}} \sum_{k=np_o}^{n_f} P(d_o > k) P \quad (\text{any } d_i \leqslant k) \tag{5.21}$$

This expression for $P(e_1)$ is very similar to that given in block coding for $P(e)_{\text{random}}$ by Eq.(A.34) of Appendix A. The situation here is somewhat more complicated, in that we now have $P(d_o > k)$

instead of $P(d_o = k)$. However, the procedure for evaluating Eq.(5.21) is much the same as in the case of block coding, which is carried through in detail in Appendix A.

First of all, we use the results of Eq.(5.8), and break the summation at $k = n_f p_t = k_t$, where p_t is defined in terms of the transmission rate R_t by Eq.(5.6). Using Eq.(5.7), we have

$$\sum_{k=np_o}^{n_f} = \sum_{k=np_o}^{k_t} \left| S_1(n_f) \right| P(d_o > k)\ P(d_i \leqslant k) + \sum_{k=k_t+1}^{n_f} P(d_o > k) \qquad (5.22)$$

The second summation is easily evaluated, by means of factoring out the leading term in $P(d_o > k)$.

$$P(d_o > k) = P(d_o = k) \frac{p_o}{q_o} \frac{n_f - k}{k + 1} \left[1 + \frac{p_o}{q_o} \cdot \frac{n_f - k - 1}{k + 2} + \ldots \right] \qquad (5.23)$$

Let

$$r_k = \frac{p_o}{q_o} \frac{n_f - k}{k + 1} \qquad (5.24)$$

Then, overbounding the bracketed series by a geometric series in r_k, we have

$$P(d_o > k) < P(d_o = k) \frac{r_k}{1 - r_k} \qquad (5.25)$$

and

$$\sum_{k=k_t+1}^{n_f} P(d_o > k) < \sum_{k=k_t+1}^{n_f} P(d_o = k) \frac{r_k}{1 - r_k} \qquad (5.26)$$

From Eq.(5.24), the largest value of $r_k/1 - r_k$ occurs when k is smallest. Evaluating this factor at $k = k_t + 1$, and removing it from under the summation, we have

$$\sum_{k=k_t+1}^{n_f} P(d_o > k) < \frac{r_{k_t+1}}{1 - r_{k_t+1}} \sum_{k=k_t+1}^{n_f} P(d_o = k) \qquad (5.27)$$

Finally, after a certain amount of algebra identical with that described in Appendix A, we obtain the bound

$$\sum_{k=k_t+1}^{n_f} P(d_o > k) < \left(\frac{p_o q_t}{p_t - p_o}\right) A_t \, 2^{-n_f E_t} \qquad (5.28)$$

The parameters A_t and E_t appear also in the block coding formulation, and their values are given in Eqs.(A.50) and (A.52).

With the help of Eq.(5.10), the first summation in Eq.(5.22) may be written in the form

$$\sum_{k=np_o}^{k_t} = \left|S_1(n_f)\right| \, 2^{-n_f} \sum_{k=np_o}^{k_t} \left[\sum_{\ell=k+1}^{n_f} P(d_o = \ell)\right] \left[\sum_{\ell=0}^{k} \binom{n_f}{\ell}\right] \qquad (5.29)$$

We factor out the largest term in the second bracketed summation, overbound by a geometric series, and recognize that the largest value of the geometric sum occurs for $k = k_t$. Exactly as in Appendix A, we then have

$$\sum_{k=np_o}^{k_t} = \left|S_1(n_f)\right| \, 2^{-n_f} \frac{1}{1 - \frac{p_t}{q_t}} \sum_{k=np_o}^{k_t} \left[\binom{n_f}{k} \sum_{\ell=k+1}^{n_f} P(d_o = \ell)\right] \qquad (5.30)$$

Since all of the values of ℓ exceed np_o, the largest term in the remaining interior sum occurs for $\ell = k+1$. We again factor out this maximum term.

$$\sum_{k=np_o}^{k_t} = \left|S_1(n_f)\right| \; 2^{-n_f} \; \frac{1}{1 - \frac{p_t}{q_t}} \; \cdot$$

$$\sum_{k=np_o}^{k_t} p_o^{k+1} \; q_o^{n_f-k-1} \binom{n_f}{k+1} \binom{n_f}{k} \left[1 + \frac{p_o}{q_o} \; \frac{n_f - k - 1}{k+2} + \ldots\right] \qquad (5.31)$$

The usual technique of overbounding with a geometric series leads to the inequality

$$\sum_{k=np_o}^{k_t} < \left|S_1(n_f)\right| \; 2^{-n_f} \; \frac{1}{1 - \frac{p_t}{q_t}} \; \sum_{k=np_o}^{k_t} p_o^k \; q_o^{n_f-k} \binom{n_f}{k}^2 \; \frac{r_k}{1 - r_k} \qquad (5.32)$$

where

$$r_k = \frac{p_o}{q_o} \; \frac{n_f - k}{k+1}$$

Finally, we once again factor the last term from the summation in Eq.(5.32), and write

$$\sum_{k=np_o}^{k_t} < \left|S_1(n_f)\right| \; 2^{-n_f} \; \frac{1}{1 - \frac{p_t}{q_t}} \; p_o^{k_t} \; q_o^{n_f-k_t} \binom{n_f}{k_t}^2 \; \cdot$$

$$\frac{r_{k_t}}{1 - r_{k_t}} \left[1 + r_c + r_c^2 + \ldots.\right] \qquad (5.33)$$

where

$$r_{k_t} = r_k\Big|_{k=k_t} < \frac{p_o}{q_o} \; \frac{q_t}{p_t} \qquad (5.34)$$

and

$$r_c = \frac{q_o}{p_o} \left(\frac{p_t}{q_t}\right)^2 \; \frac{1 + q_o/n_f(p_t - p_o)}{1 - p_o/n_f(p_t - p_o)} \qquad (5.35)$$

Equation (5.33) exhibits the same kind of "critical" behavior that occurs in block coding. The critical rate of transmission is defined in Appendix A to be

$$R_{crit} = 1 - H(p_{crit}) \qquad (A.65)$$

where p_{crit} is the solution to

$$\frac{p_{crit}}{q_{crit}} = \sqrt{\frac{p_o}{q_o}} \qquad (q_{crit} = 1 - p_{crit}) \qquad (A.46)$$

Although Eq.(5.35) would indicate a slight increase in the critical rate for sequential decoding, we expect that this is a result of approximations incident to the analysis, and not of the actual decoding procedure itself. In any event, this shift is asymptotically zero as the convolutional constraint span n_f goes to infinity, and is negligible in the practical case of large n_f.

In order to avoid unnecessary complication in the form of our results, we neglect the apparent displacement of p_{crit}, and consider only the asymptotic case. Then, when $R_t < R_{crit}$, the geometric sum in r_c converges. For $R_t \geq R_{crit}$, on the other hand, we may bound the summation by the product of the largest term (which occurs at $k = n_f p_{crit}$) and the number of terms. The situation is again exactly analogous to that in block coding. The final results, using the notation of Appendix A, are as follows:

$$\left.\begin{aligned} \sum_{k=np_o}^{k_t} &\lesssim \frac{1}{2}\left(\frac{p_o q_t}{p_t - p_o}\right) A_r \, 2^{-E_t} && (\text{for } p_t < p_{crit}) \\ &\lesssim \frac{1}{2}\left(\frac{p_o q_t}{p_t - p_o}\right) A_{crit} \, 2^{-E_{crit}} && (\text{for } p_t \geq p_{crit}) \end{aligned}\right\} \qquad (5.36)$$

The symbol "$\lesssim$" is used above to represent an inequality that is only asymptotically rigorous. The parameters A_r, A_{crit}, and E_{crit} are defined in Appendix A by Eqs.(A.49), (A.51), and (A.53), respectively.

It is most convenient to collect the results of Eqs.(5.28) and (5.36) into an expression that bounds the ensemble average sequential decoding probability of error $P(e_1)$ in terms of the corresponding bound for block coding, $P(e)_{random}$. Let

$$A_S = \frac{p_o q_t}{p_t - p_o} \cdot \left(\frac{1}{B}\right)^{1/1-B} \tag{5.37}$$

where B is defined in Eq.(4.18) as $\frac{CR_t/E_m}{C - R_t}$. Then, referring to Eqs.(5.20), (A.54), and (A.55), we have the final result

$$P(e_1) \lesssim n_f A_S P(e)_{random} \tag{5.38}$$

Discussion. The bound on the ensemble average probability of error for sequential decoding given by Eq.(5.38) is asymptotically rigorous in the limit of large n_f for any rate of transmission R_t less than the channel capacity C. However, the corresponding bound on the average number $(\bar{N})$ of computations required to eliminate the subset S_1 of incorrect messages, as determined in Chapter IV, converges only for values of the parameter B that are less than unity. Accordingly, we expect the decoding procedure itself to be useful only for rates of transmission such that

$$R_t < \frac{C}{1 + C/E_m} \tag{4.25}$$

where

$$E_m = \left(\frac{1}{2} - p_o\right) \log \frac{q_o}{p_o} - C \tag{B.5}$$

The ways in which the sequential decoding technique that we are investigating degrades the probability of error behavior is apparent from Eq.(5.38). Elias[4] shows that the maximum-likelihood average probability of error for convolutional coding is bounded by $P(e)_{random}$. The result for $P(e_1)$ exceeds this bound by the product of three coefficients.

First, the factor n_f enters into the computation on account of the fact that the transmitted sequence s_o is observed by the decoding computer at every different length n, and therefore runs the risk of being discarded n_f distinct times. In practice, of course, this effect is somewhat ameliorated: if s_o is retained at length n, it is less likely to be summarily discarded at length $(n+1)$ than it would be if no prior measurement had been made.

Second, the decoding computer searches through the truncated message set S_f using distance criteria $(k_n)_j$ which increase with j in increments greater than unity. Accordingly, in Eq.(5.11) the "weighting" factors Q(j) [the probabilities that the search procedure terminates at the j^{th} stage] are each degraded by $2^{\Delta K}$ over the corresponding maximum-likelihood value. This introduces the factor $\left(\frac{1}{B}\right)^{1/1-B}$ into the coefficient A_S in Eq.(5.37).

Third and last, the distance criteria k_n are determined by Eq.(4.1) to be such that $P(d_o > k_n) = 2^{-K}$. The appropriate maximum-likelihood procedure would call for $P(d_o = k_n) = 2^{-K}$. This accounts for the factor $\frac{p_o q_t}{(p_t - p_o)}$ in A_S.

Of these three effects, only the one involving n_f is significant, in terms of the encoding constraint length n_f required to

obtain a given standard of performance. Essentially, degradation of the probability of error by a factor n_f is the price paid for reduction of the number of decoding computations.

Since $P(e)_{random}$ is shown in Appendix A and Chapter II to be an exponentially decreasing function of message length, even the coefficient n_f in the expression for $P(e_1)$ is relatively unimportant. In order to design for a given probability of error, the magnitude of n_f need not be increased greatly over that value required for block coding.

Furthermore, as mentioned in Chapter II, the average error behavior of all block codes is exponentially optimum in the limit of large code length. Accordingly, the proposed sequential encoding-decoding procedures are also exponentially optimum, whenever an extremely small probability of error is required.* It should be mentioned, however, that the departure from optimum behavior is actually by the square of n_f. This follows from the fact that sequentially only one digit of the information sequence is determined at a time. In optimum block coding, on the other hand, the computed probability of error relates to an entire transmitted sequence of length n_f.

The quantity $P(e_1)$ bounded in Eq.(5.38) is defined as the average probability of error per digit, over the ensemble of all possible generator sequences g. As usual, we expect most choices for g to be substantially optimum. Finally, we note that it should not be difficult to find convolutional generator sequences for which both the probability of error and the number of decoding computations

*These results apply, of ccurse, only for rates of transmission greater than critical.

are simultaneously representative of the ensemble average. The same distance relations among the sequences in the convolutional message set that minimize the error rate serve also to reduce the requisite number of computations.

The bound on the average probability of error given in Eq.(5.38) applies only when no prior errors have been committed. The decoding procedure depends upon the ability of a digital computer to generate the entire truncated set S_f of all possible messages of length n_f that are consistent with the part of the transmitted sequence which is already decoded. So soon as the receiver once does make an error, this complete set S_f becomes totally "incorrect." Since this condition, once established, perpetuates itself thereafter, the sequential decoding procedure can provide not only exponentially optimum error correction, but also virtually perfect error detection.

Whether or not this inherent feature is desirable would seem to depend both upon the possible application and upon the actual value of the probability of error. For values of $P(e_1)$ of the order of 10^{-10} or less, knowledge that an error had in fact been made would appear to be advantageous.

CHAPTER VI

COMPUTATION CUT-OFF LEVELS

1. Nature of the Problem

In accordance with the rules stipulated in Chapter IV, the decoding computer searches through the truncated message set S_f, using the smallest untried probability criterion K_j, until either

(a) any message is retained to length n_f , or

(b) the entire set S_f is discarded as improbable.

If set S_f is completely discarded, the computer starts over again from the beginning, using the next-larger criterion K_{j+1}.

With these rules, the decoding procedure terminates when, and only when, some message <u>is</u> retained to length n_f, for some K_j. An error, of course, occurs whenever this retained sequence is a member of the incorrect subset S_1. The ensemble average probability of this kind of error is calculated in Chapter V, and is designated $P(e_1)$.

The form of the set of probability criteria is also specified in Chapter IV and Appendix C.

$$K_j = K_1 + (j-1)\Delta K \qquad (C.22)$$

The arbitrary parameters K_1 and ΔK are determined so as to minimize the upper bound on the average number of binary computations required to eliminate the subset S_1, where the averaging is over the ensemble of possible convolutional generator sequences. It is for these minimizing values of K_1 and ΔK that the average probability of error $P(e_1)$ is calculated.

In none of the above do we give consideration to the number

of computations which must be made concurrently upon the correct subset S_o. It is possible that many sequences in S_o might lie close to the received message over a considerable length $n < n_f$, and ultimately become improbable according to criterion K_j only as n approaches n_f. Since S_o, as well as S_1, contains an exponentially large number of sequences, the decoding computer could conceivably make an enormous number of computations without reaching the decision to print, even for small values of j.

The probability of such an eventuality is difficult to analyze on account of the statistical dependencies between S_o and the received message. On the other hand, the ensemble average behavior of the incorrect subset S_1 is analyzed rigorously in Appendix C — and we can program the decoding computer to take special note of particularly untypical departures from this mean.

Let $\overline{N}_j$ designate the ensemble average number of computations required to eliminate S_1 when $K = K_j$. If, in a particular experiment, many more than $\overline{N}_j$ computations are made upon a specific but unidentified subset without discarding it completely, then we can infer that this subset is very unlikely to be S_1. Conversely, it becomes correspondingly probable by elimination that this unidentified subset is S_o.

2. Probability of Error

In order to take advantage of this difference in the statistical behavior of subsets S_o and S_1, it is reasonable to modify the decoding rules established in Chapter IV, as follows:

(a) For the smallest untried criterion K_j, the computer searches progressively through the entire message set S_f, operating about equally upon both subsets.

(b) So soon as any sequence is retained to length n_f, it prints the corresponding first information digit.

(c) If no sequence is retained, the computer continues to search equally through both subsets until one of them is completely discarded.

(d) The computer then operates exclusively upon the remaining subset, until one of the following three mutually exclusive events occurs.

1. This second subset also is completely eliminated. Then the computer begins the search anew, using criterion K_{j+1}.

2. A sequence is retained to length n_f. In this case the computer prints the corresponding first information digit.

3. A total of L_j binary computations is made upon this remaining subset. In this case also, the computer prints the (common) first information digit of the subset.

L_j is thus a computation cut-off level, which is introduced into the decoding rules in order to obviate the possible occurrence of a near-interminable process. When the procedure above is adopted, however, a new and distinct type of possible error is introduced concomitantly. An error will result whenever both the correct message subset S_o is discarded for K_j, and L_j computations fail to eliminate S_1.

Designate the average probability of this second kind of error as $P(e_2)$. In order that the over-all average probability of error be relatively unaffected by the modified decoding procedure, we

wish to determine the set of cut-off levels L_j so that

$$P(e_2) \leqslant P(e_1) \tag{6.1}$$

In Eq.(6.1), $P(e_1)$ is an average probability of error, over the ensemble of all 2^{n_f} possible convolutional generator sequences. We consider $P(e_2)$ to be this same sort of an ensemble average probability.

In practice, we are of course interested in establishing the existence of a <u>particular</u> code whose error attributes are representative of the ensemble with respect both to e_1 and to e_2. We again apply Shannon's argument. Only $1/\rho$ of the generators can give codes whose error behavior is as bad as $\rho P(e_1)$ with respect to e_1, and by the same token only $1/\eta$ can give codes as bad as $\eta P(e_2)$ with respect to e_2. Therefore at least $(1 - 1/\rho - 1/\eta)$ of the possible generator sequences must produce code sets whose probability of error for e_1 and e_2 is simultaneously no worse than $\rho P(e_1)$ and $\eta P(e_2)$. As an example: if $P(e_1) = P(e_2) = 10^{-12}$ and $\rho = \eta = 10$, then at least 80 per cent of the 2^{n_f} convolutional generators produce codes whose over-all probability of error is at most $2 \cdot 10^{-11}$.

As in the case of $P(e_1)$, we can also determine an upper bound to $P(e_2)$ by means of averaging first over the ensemble of generator sequences, and then over the ensemble of transmission errors. Given a criterion K_j, the probability of a second-type error is bounded by

$$P_j(e_2) \leqslant P_j(s_o \text{ discarded}) P(N_j > L_j) \tag{6.2}$$

where N_j is the actual number of binary computations required in a particular experiment to completely eliminate the incorrect subset S_1,

and s_o is the transmitted message. Equation (6.2) follows directly from the modified decoding rules: at worst, both elimination of the correct message and failure to eliminate S_1 completely are conditions necessary to an error of the second type, and these events are statistically independent over the ensemble of transmission errors.

Next we sum over j. Then

$$P(e_2) \leqslant \sum_j P_j(s_o \text{ discarded})\ P(N_j > L_j) \tag{6.3}$$

Through evaluation of Eq.(6.3), we next show that the condition of Eq.(6.1) is satisfied when

$$P(N_j > L_j) = P(e_1), \quad \text{for all } j. \tag{6.4}$$

In Appendix C, we establish that

$$P_j(s_o \text{ discarded}) \leqslant n_f 2^{-K_j} \tag{C.24}$$

Substituting Eqs.(6.4), (C.24), and (C.22) into Eq.(6.3), and summing, we obtain the inequality

$$P(e_2) \leqslant \frac{n_f}{1 - 2^{-\Delta K}}\, 2^{-K_1}\, P(e_1) \tag{6.5}$$

The values of K_1 and ΔK which minimize the bound on the ensemble average number of binary computations necessary to eliminate S_1 are given in Eqs.(C.30) and (C.31). Substituting into Eq.(6.5),

$$P(e_2) \leqslant \frac{1}{\left(\frac{1}{B}\right)^{1/1-B} - 1}\, P(e_1) \tag{6.6}$$

In the limit as B approaches unity from below, $\left(\frac{1}{B}\right)^{1/1-B}$ approaches the natural base e from above. Accordingly, we have finally the

inequality

$$P(e_2) \leq \frac{1}{e-1} P(e_1) < P(e_1) \qquad (6.7)$$

Since the probability of a union of events can be no greater than the sum of the constituent probabilities, it follows that the over-all ensemble average error probability for the modified sequential decoding procedure is bounded by $P(e_1)$ plus $P(e_2)$. When Eq.(6.4) is satisfied, the final result after simplification is

$$P(e)_{\text{sequential}} < 1.59\, P(e_1) \qquad (6.8)$$
$$\text{(for } B < 1\text{)}$$

3. Estimate of Cut-Off Levels

The problem of rigorously evaluating the set of cut-off levels L_j in accordance with Eq.(6.4) is made difficult by the statistical interdependencies which exist between the messages in the incorrect subset S_1. On the other hand, if these dependencies are disregarded, a tractable but inexact mathematical analysis is possible.

Approximate Analysis. Although assuming that for each value of n the $\left|S_1(n)\right|$ sequences of length n in S_1 are all statistically independent of each other is clearly incorrect, we can show heuristically that making such an assumption is not totally unreasonable. As is illustrated in Fig. (4.1), the sequences in S_1 are mutually constrained so as to form a tree-structure. Using the concepts of n-dimensional geometry, we think of a binary sequence as defining the co-ordinates of a point. Thus the sequence 10110 .... specifies the point reached by moving 1 unit along axis 1, 0 units along axis 2, 1 unit along axis 3, and so on.

This concept lends a direct geometrical significance, without

change of meaning, to such terms as "distance," which in Chapter II is defined simply as the number of digits (co-ordinates) in which two sequences differ. Similarly, the term "direction" has a clear geometrical interpretation, in terms of a vector drawn between two points. Using these notions, we can think of the tree-structure of the convolutional subset S_1 as constraining the message points to be "clustered" together in n-space.

For "good" choices of the convolutional generator sequence - that is, choices for which the actual value of the probability of error is characteristic of the ensemble - we expect the clusters of sequences in S_1 to be directed away from the supposed transmitted sequence of all 0's. By this, we mean that about one half of the digits in every sequence of length n in S_1 are expected to be 1's. Furthermore, since the actual error probability will be small whenever it is characteristic, we expect that the clusters of S_1 will also be directed substantially away from the received message, for most of the more probable noise perturbations.

At this point it is well to recall that the cut-off levels L_j are introduced into the decoding procedure not to guard against misbehavior of the incorrect subset S_1, but rather to obviate possible difficulties with S_0. We are seeking to protect the computer primarily against transmission error patterns which are not necessarily unlikely, but which cause the received message to be barely improbable with respect to one of the (smaller) criteria K_j.

For really large values of K_j, the use of which implies extraordinarily improbable noise sequences, we expect the incidence of decoding

errors of type e_1 to be high anyway. It is, accordingly, of less concern that in these unlikely circumstances errors of type e_2 may encroach more rapidly than estimated, because of faulty determination of L_j.

Now consider a particular convolutional code, which we are free to assume is one of the many representative good ones. To reiterate, by this we mean that averages and probabilities computed for this one code over the set of possible transmission error patterns are nearly equal to those computed over the ensemble of all 2^{n_f} possible convolutional codes of the same form. For convenience of notation, we prime all quantities pertaining to the specific code under consideration.

For this chosen good code, the condition that is equivalent to the requirement on the ensemble posed by Eq.(6.4) is

$$P'(N'_j > L_j) = P'(e_1), \quad \text{for all } j \tag{6.9}$$

where these probabilities are now computed over the set of transmission errors. In order to determine L_j, we use a procedure similar to that used in Chapter IV to determine $\bar{N}_K$. Let $M'_j(n)$ represent the actual number of different sequences of length n belonging to the incorrect subset S_1 that are probable according to criterion K_j in a particular experiment performed with the selected code set. Then a function $\lambda_j(n)$ exists, such that over the ensemble of transmission error patterns,

$$P'\left[M'_j(n) > \lambda_j(n)\bar{M}'_j(n)\right] = P'(e_1) \text{ , for all n.} \tag{6.10}$$

If we can solve Eq.(6.10) for $\lambda_j(n)$, we can specify an L_j to satisfy Eq.(6.9).

For the chosen representative good code, by definition $P'(e_1) \approx P(e_1)$ and $\overline{M}'_j(n) \approx \overline{M}_j(n)$. Therefore Eq.(6.10) is significantly equivalent to requiring that

$$P'\left[M'_j(n) > \lambda_j(n)\overline{M}_j(n)\right] = P(e_1) \text{ , for all } n. \qquad (6.11)$$

In accordance with the foregoing discussion, we are particularly concerned with a partial ensemble consisting of the more probable transmission error patterns only. We can define probabilities measured over this partial ensemble, and distinguish them by a double-prime notation. When the parameters are left unchanged, but the ℓ.h.s. probability is measured over the partial error-pattern ensemble, direct rewriting of Eq.(6.11) is conservative. For the $\lambda_j(n)$ that satisfies Eq.(6.11),

$$P''\left[M'_j(n) > \lambda_j(n)\overline{M}_j(n)\right] \leqslant P(e_1) \qquad (6.12)$$

On the other hand, a value of $\lambda_j(n)$ for which Eq.(6.12) holds true of course does not necessarily satisfy the original requirement of Eq.(6.10). In situations of interest, however, on account of the considerations presented above it is reasonable to hope that determining L_j on the basis of such a $\lambda_j(n)$ does not seriously alter the over-all error behavior of the decoding scheme. This follows from the fact that the conditions implied for Eq.(6.12) — a good convolutional code, and an ensemble of the more probable transmission error patterns only — are exactly those which are of greatest practical importance.

Unfortunately, it is apparently still not possible to solve Eq.(6.12) for the appropriate functions $\lambda_j(n)$. A somewhat related

problem, however, can be stated by disregarding the constraints between the $\left|S_1(n)\right|$ sequences of length n in the incorrect subset S_1.

Consider a block code of the same length n, containing the same number of sequences $\left|S_1(n)\right|$, each of which, however, has been selected independently at random. Over the ensemble of all possible such random block codes, it is shown in Appendix D that the average number of these sequences that are probable according to criterion K_j is also $\bar{M}_j(n)$, a result which is completely independent of the received sequence.

Furthermore, we can determine a function $\lambda_j^*(n)$ by requiring that

$$P_r\left[M_j(n) > \lambda_j^*(n)\bar{M}_j(n)\right] \leqslant P(e_1) \tag{6.13}$$

where the ℓ.h.s. probability is measured over the ensemble of random block codes of length n, as indicated by the subscript r.

Let us compare the situations envisioned in Eqs.(6.12) and (6.13). In the first case, we have $\left|S_1(n)\right|$ messages arranged on a tree, where the clusters of the tree are directed away from the received sequence. In the second case, we have the same number of messages, each of which is chosen independently and at random with respect to any particular received sequence. The two structures are manifestly different. At the same time, however, there seems to be no apparent reason why the probable-message behavior of the good tree-set over a restricted ensemble of the more likely noise sequences should be remarkably inferior to that of the block-set over the ensemble of all possible random sequence selections. We can think of the good-code requirement as constraining the stems

of the tree sequences to lie distant from the received message in those cases of primary importance, whereas with random selections one takes his chances.

With this background of heuristic reasoning, we proceed to determine L_j in terms of that unknown $\lambda_j(n)$ which satisfies Eq. (6.11). In order to obtain a numerical evaluation, we then substitute for $\lambda_j(n)$ the function $\lambda_j^*(n)$ obtained from solution of Eq.(6.13). It is reasonable to hope that this procedure can yield insight into the actual characteristics of these computation cut-off levels.

Estimation of L_j. Assume that $\lambda_j(n)$ has been chosen to satisfy Eq.(6.11). Then, with probability $1 - P(e_1)$, there are no more than $\lambda_j(n)\overline{M}_j(n)$ messages of length n in S_1 that are probable with respect to criterion K_j. As is pointed out in Chapter IV and Appendix C, the decoding computer need generate only $\Delta(n)$ new binary digits for each probable message in S_1 of length n, in order to progress to length $(n+1)$. $\Delta(n)$ equals 2 or 1 , depending upon whether or not n corresponds to a node in the tree-structure of Fig. 4-1.

Let us establish the value of L_j by Eq.(6.14).

$$L_j = \sum_{n=1}^{n_f} \Delta(n)\lambda_j(n)\overline{M}_j(n) \tag{6.14}$$

Then it follows that

$$P'(N_j' > L_j) \leqslant P(e_1) \approx P'(e_1) \tag{6.15}$$

since $M_j'(n)$ must exceed $\lambda_j(n)\overline{M}_j(n)$ for at least one value of n if N_j' is to exceed L_j.

We obtain the estimate L_j^* of L_j by replacing $\lambda_j(n)$ in Eq. (6.14) by $\lambda_j^*(n)$, where $\lambda_j^*(n)$ satisfies Eq.(6.13).

$$L_j^* = \sum_{n=1}^{n_f} \Delta(n)\lambda_j^*(n)\overline{M}_j)n) \qquad (6.16)$$

Detailed consideration of the estimated cut-off levels L_j^* is carried out in Appendix D. It is shown there that L_j^* increases less rapidly than the square of the code length n_f. We define the mean estimated computation cut-off level $\overline{L}^*$ to be the average value of L_j^*, with respect to the probability that a criterion K_j is actually utilized in the process of decoding. It is shown in Appendix D that $\overline{L}^*$ also increases no faster than the square of n_f.

In order to obtain actual numbers L_j^*, we must resort to numerical methods. For the case of $p_o = .050$, $R_t = 1/3$, and $P(e_1) = 10^{-12}$, the ratio of L_j^* to the bound on $\overline{N}_j$ is plotted in Fig. 6-1. As in Chapter IV, $\overline{N}_j$ is the average number of binary computations required to eliminate the incorrect subset S_1 with respect to criterion K_j, where the averaging is over the ensemble of all possible convolutional generator sequences. It is seen that the ratio $L_j^*/(\overline{N}_j)_{bound}$ is not unattractively large, and that it decreases slowly with increasing j.

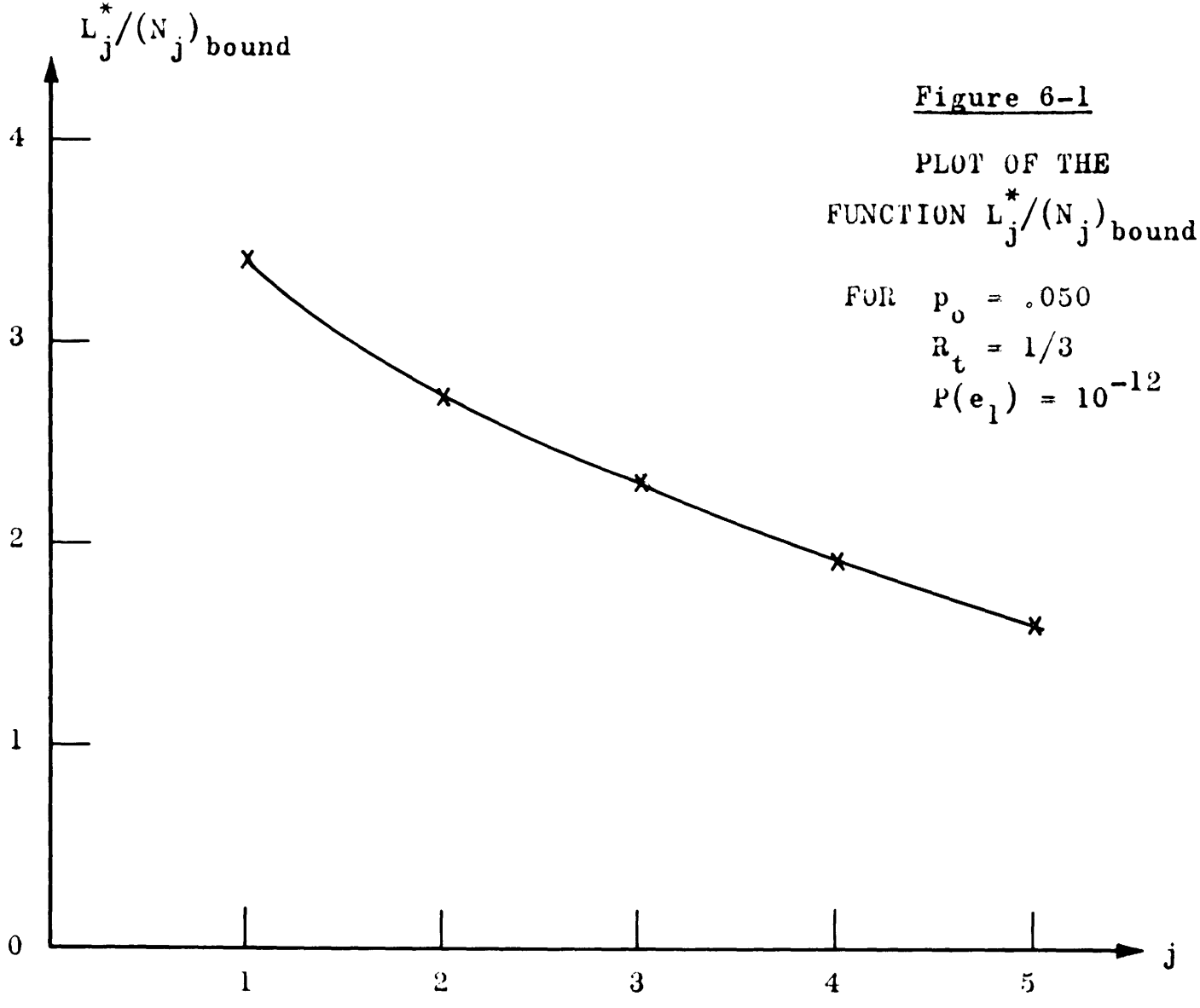

Figure 6-1

PLOT OF THE FUNCTION $L_j^*/(N_j)_{bound}$

FOR $p_o = .050$
$R_t = 1/3$
$P(e_1) = 10^{-12}$

CHAPTER VII

DISCUSSION

1. Summary of Results

Shannon's fundamental theorem[1] for noisy channels states that it is possible to communicate over such a channel, at any constant information rate less than capacity, with an arbitrarily small (non-zero) probability of error. Ever since 1948, when this theorem was first published, this intriguing possibility has been the subject of a great deal of research.

Generally speaking, the results of this research may be divided into two categories. Hamming,[6] Reed,[9] Slepian,[10,15] and others have devised codes for the Binary Symmetric Channel that are optimum in special instances, and for which practicable decoding procedures exist. These codes do not, however, provide for the transmission of information at a non-zero rate, when the decoding probability of error is required to decrease indefinitely. On the other hand, Feinstein,[8] Shannon,[2,3] and Elias[4,5] have investigated the general properties of constant-information-rate codes, and have shown that such codes exist for which the probability of error decreases exponentially with increasing code-word length n_f. The decoding problem for this case has not been previously investigated, beyond pointing out that the brute-force, maximum-likelihood procedure involves a number of computations that increases exponentially with n_f. Finally, Elias[12] has suggested an iterative code that provides arbitrarily high reliability at a positive rate of information transmission. The limitations are that the transmission rate

cannot approach the channel capacity, and that the decoding probability of error approaches zero as a function of delay more slowly than it should.

The code considered in this report is another step towards bridging the gap between theory and practice. Convolutional coding permits communication, with arbitrarily high reliability, over a noisy binary symmetric channel. For rates of transmission R_t greater than critical, the probability of error can be caused to decrease in an exponentially optimum way.

The average number of decoding computations is introduced as an additional parameter. In the proposed sequential decoding procedure, this number of computations converges for values of R_t less than $\frac{C}{1 + C/E_m}$, which is greater than R_{crit} for channel transition probabilities $p_o > .0015$. Whether the procedure itself, or only the bound on the average number of computations, diverges as R_t approaches closer to the capacity C is not yet known. The procedure obviously has a limit of looking at everything.

The probability of error and the number of decoding computations, considered separately, are each well behaved. Unfortunately, it has not as yet been possible to prove rigorously that the decoding procedure converges simultaneously as the probability of error is reduced indefinitely towards zero. It appears reasonable, however, that such should be the case.

Probability of Error. The non-rigorous portion of this report concerns the determination, in Chapter VI, of appropriate computation cut-off levels L_j. These levels are introduced into the problem in order to obviate the possibility of a near-interminable decoding process. If, for the moment, we neglect both the necessity for these cut-off levels and their effect, then the ensemble average probability of error for sequential decoding is asymptotically

bounded in Chapter V for large values of n_f by

$$P(e_1) < n_f A_S P(e)_{random} \tag{5.38}$$

where n_f is the span of the convolutional constraints imposed by the encoding computer. The coefficient A_S is a function only of the BSC transition probability p_o and the rate of information transmission R_t.

$$A_S = \frac{p_o q_t}{p_t - p_o} \cdot \left(\frac{1}{B}\right)^{1/1-B} \tag{5.37}$$

where

$$R_t = 1 - H(p_t) \tag{5.6}$$

and

$$B = \frac{CR_t/E_m}{C - R_t} \tag{4.18}$$

The factor $P(e)_{random}$ is defined as the average probability of error over the ensemble of all possible block codes of length n_f. It is shown in Chapter II and Appendix A that this average behavior of all codes is exponentially optimum, in the limit of large code length, for rates of transmission greater than critical. Since $P(e_1)$ is degraded only by the linear coefficient n_f, this exponential optimality is also true of sequential decoding.

Upper bounds on $P(e)_{random}$ are given in Eqs.(A.54) and (A.55). The essential characteristic is that the attainable probability of error decays exponentially with increasing length n_f.

$$P(e)_{random} < A\, 2^{-n_f E} \tag{7.1}$$

where A and E are appropriate constants, depending only on the channel capacity C and the transmission rate R_t.

Typical plots of the required encoding constraint length n_f, as a function of the ensemble average probability of error, are given in Fig. 7-1 for sequential and block decoding. It is seen that, at the error rates considered, the performance of the sequential system is not intolerably inferior.

In order to illustrate the magnitudes involved, for a 100-words-per-minute teletype system a probability of error of 10^{-6} is equivalent to approximately one error each 6 hours of operation. A probability of error of 10^{-12} corresponds to one error each 6 centuries. For the example shown, $p_o = .050$ and $R_t = 1/3$. If we assume (admittedly incorrectly for an actual communications channel) that p_o is independent of the pulse duration, the uncoded error rate would be one per second. Finally, the inherent delay of $n_f = 345$ pulses, introduced for $P(e_1) = 10^{-12}$ by the sequential decoding procedure, amounts to approximately one third of a line of text.

For sequential decoding, typical behavior of n_f with respect to variations in the transmission rate R_t and channel transition probability p_o are illustrated in Fig. 7-2. As would be expected, when the decoding error probability is held constant, the required code length n_f increases both with R_t and with p_o.

Finally, it is shown in Chapter VI that the computation cut-off levels L_j, whose effect we have neglected thus far, can in principle be so assigned that the total probability of error $P(e)_{sequential}$ is relatively unaffected.

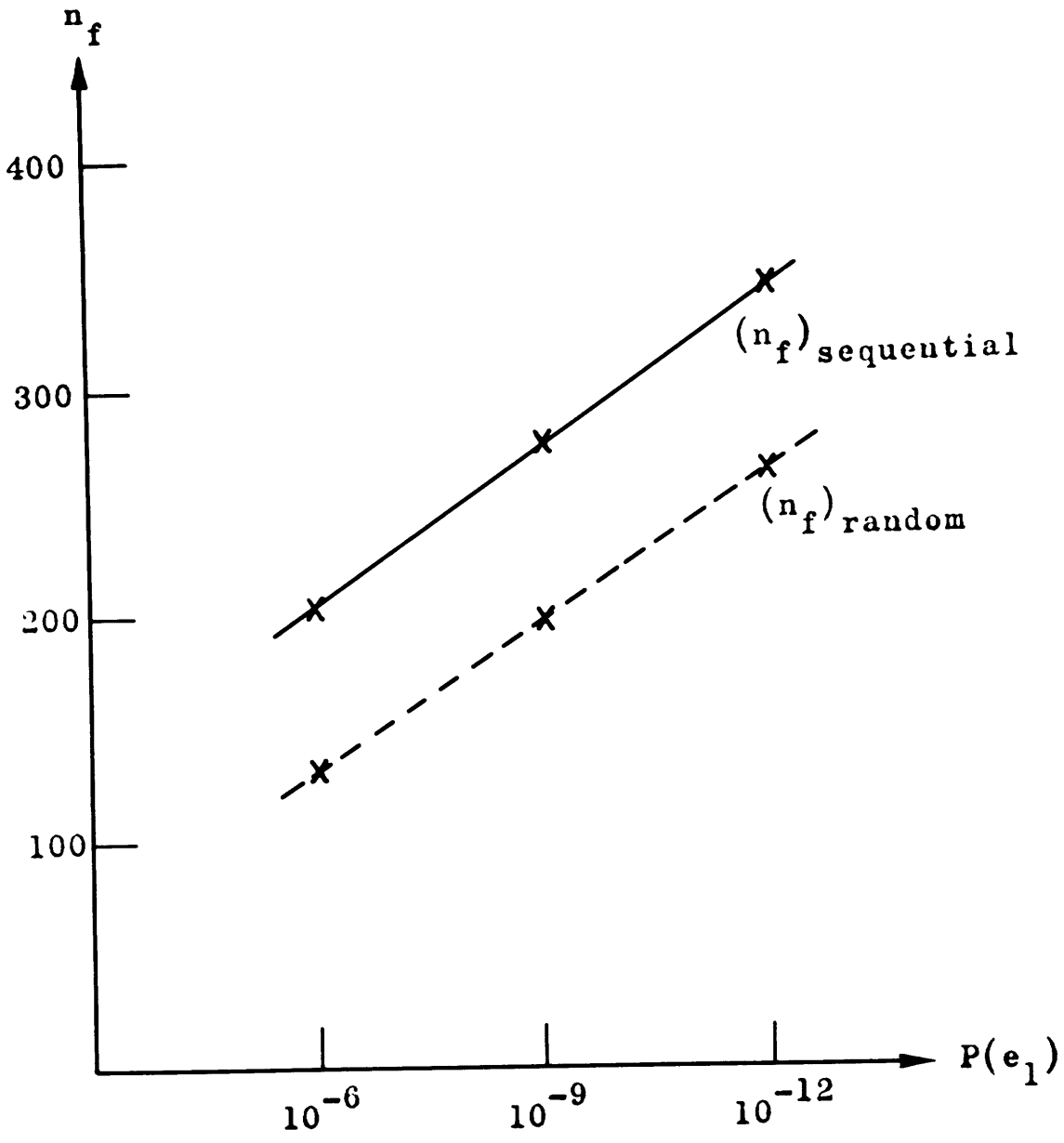

Figure 7-1

PLOT OF SEQUENCE LENGTH AGAINST PROBABILITY OF ERROR FOR $p_o = .050$, $R_t = 1/3$

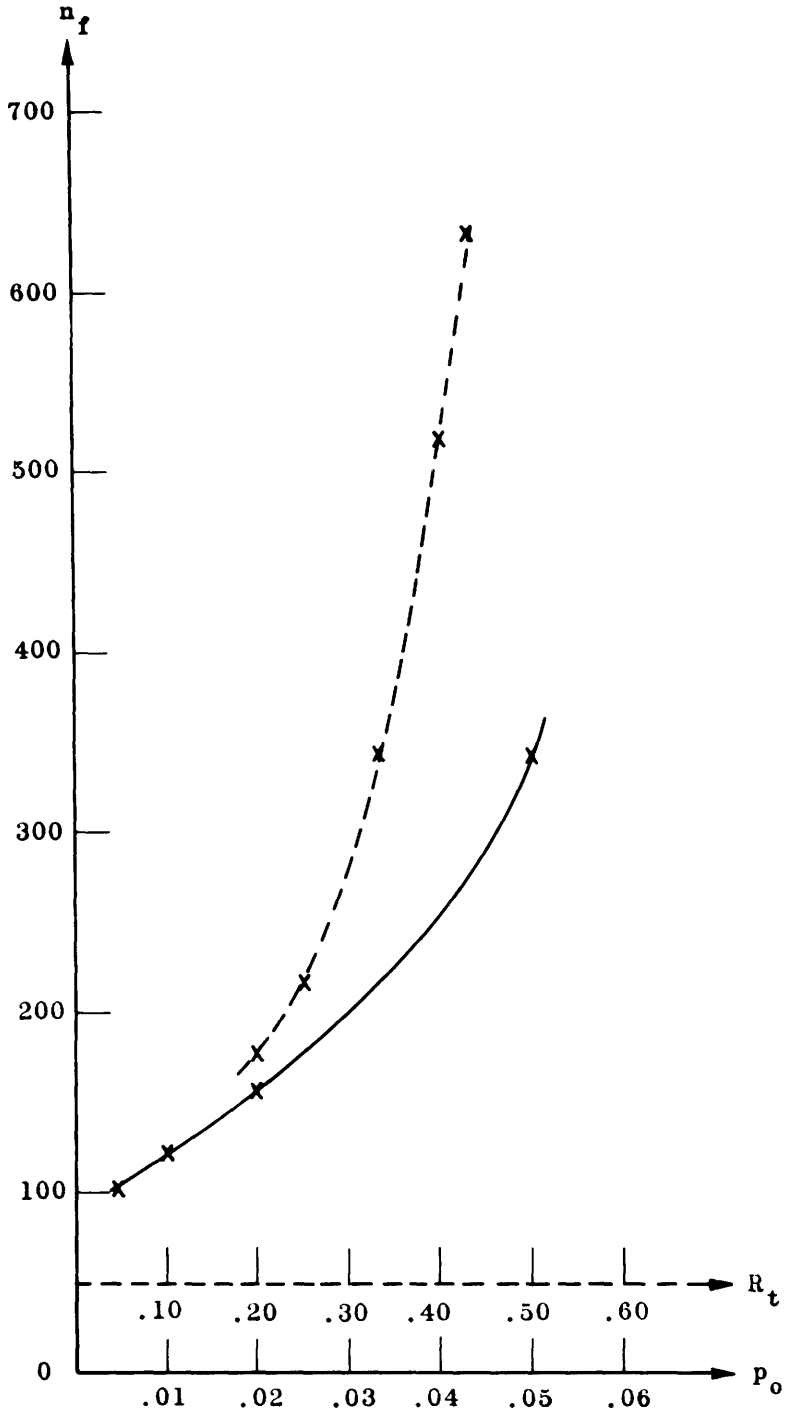

Figure 7-2

PLOT OF n_f AGAINST R_t, FOR p_o = .050 AND $P(e_1) = 10^{-12}$
PLOT OF n_f AGAINST p_o, FOR R_t = 1/3 AND $P(e_1) = 10^{-12}$

$$P(e)_{\text{sequential}} \leq 1.59\ P(e_1) \qquad (6.8)$$

As is pointed out in that chapter, however, no reasonable way of rigorously bounding the values of L_j that are required in order to satisfy Eq.(6.8) has yet been discovered.

Whether or not the estimated values L_j^*, computed in Appendix D, will suffice is open to debate. The probabilities with which we are concerned are so extremely small that intuition and heuristic reasoning are even further removed than usual from infallibility. From a practical point of view, it might likewise be argued that these probabilities are also so small as to make the question academic. The author personally feels that the estimated values are at least sufficiently close to being correct that an experiment is not likely to disprove their validity. However, the problem is of enough theoretical interest to be important in its own right, and deserves further investigation.

Number of Decoding Computations. An upper bound to the average number $(\overline{N})$ of binary computations that are required in order to discard every possible message sequence corresponding to an incorrect decoding decision is given by Eq.(C.34) in Appendix C. It follows, from minimization of this bound, that

$$\overline{N} \approx D_5\ n_f^B \sqrt{\log D_6 n_f} \qquad (\text{for } B < 1) \qquad (C.35)$$

where D_5 and D_6 are constants determined by the BSC and transmission rate only. As mentioned in Chapter IV, this is a far more tractable behavior than the exponential growth that is characteristic of the general maximum-likelihood decoding procedure. We have already mentioned that the price paid for this improvement is degradation

of the probability of error by the factor $n_f A_S$.

Plots of the variation of the bound on $\bar{N}$ with respect to $P(e_1)$ and p_o, computed from Eq.(C.34), are given in Fig. 7-3. The slow increase in $\bar{N}$ with $P(e_1)$, and hence n_f, is particularly noticeable. The more rapid variation with respect to p_o is attributable to changes in the parameter $B = \frac{CR_t/E_m}{C - R_t}$. When R_t is held constant, increasing p_o causes C to decrease and B to approach unity.

As is pointed out in Chapter IV, the proposed decoding scheme is guaranteed to converge only for values of $B < 1$, which corresponds to a transmission rate

$$R_t < \frac{C}{1 + C/E_m} \qquad (4.25)$$

This follows from the fact that, when $B < 1$, the bound on the average number of computations required in decoding increases too rapidly. This sensitivity of $\bar{N}$ with respect to the transmission rate is dramatically evident in Fig. 7-4, which is plotted to a semi-logarithmic scale. However, even though the bound on $\bar{N}$ becomes infinite as R_t increases, it can be argued as well that its magnitude is quite reasonable for smaller, but still substantial, transmission rates.

By means of the introduction of the computation cut-off levels L_j, it is possible to bound the total average number of decoding computations required per information digit. Let this total average be represented by $\bar{N}_f$, and let $\bar{L}$ be defined as the average value of L_j, with respect to the probability that criterion K_j is used in the decoding procedure.

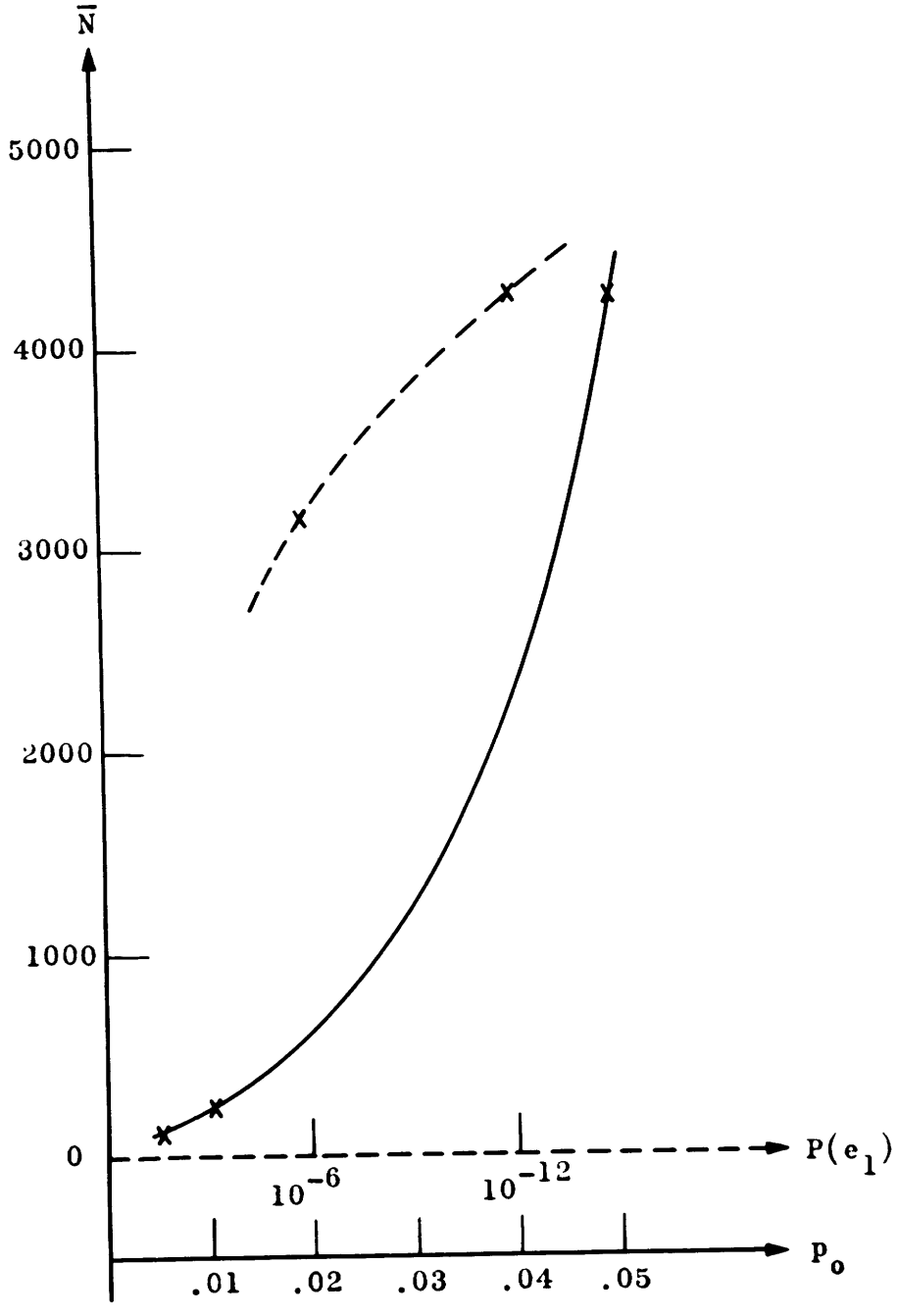

Figure 7-3

PLOT OF $\bar{N}$ AGAINST $P(e_1)$, FOR $R_t = 1/3$ AND $p_o = .050$
PLOT OF $\bar{N}$ AGAINST p_o, FOR $R_t = 1/3$ AND $P(e_1) = 10^{-12}$

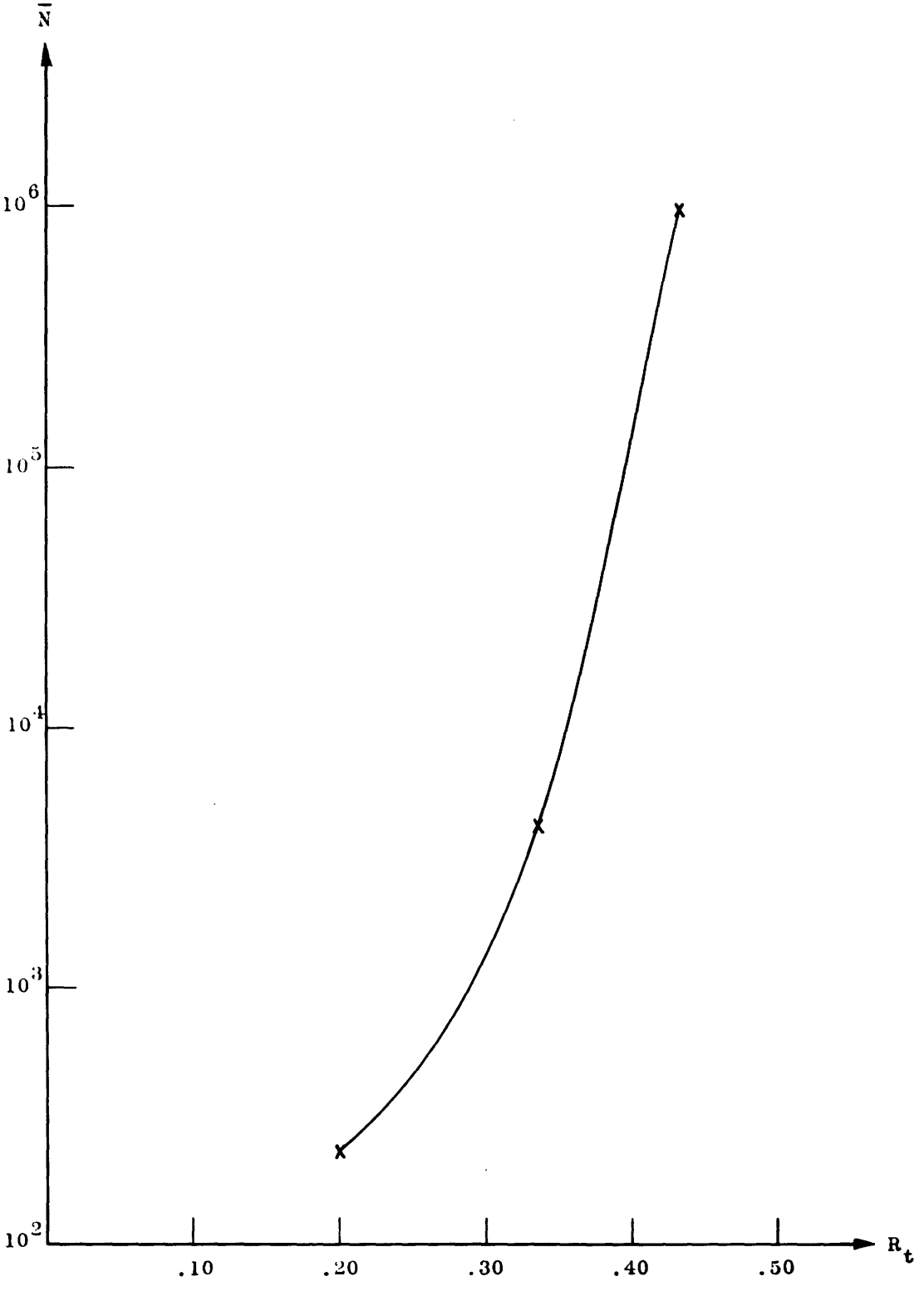

Figure 7-4

PLOT ON $\bar{N}$ AGAINST R_t, FOR $p_o = .050$ AND $P(e_1) = 10^{-12}$

$$\bar{L} = \sum_j P(j)\, L_j \tag{7.2}$$

The quantity $\bar{L}$ then provides an upper bound to the average number of binary computations performed upon that subset of all possible messages consistent with a correct decoding decision. Since the average computational effort for the incorrect subset is bounded by $\bar{N}$, it follows that

$$\bar{N}_f \leq \bar{L} + \bar{N} \tag{7.3}$$

In so far as the behavior of the estimated cut-off levels L_j^* is representative of the actual values L_j, we expect that $\bar{L}$ need not be very much larger than $\bar{N}$. This follows from the plot of $L_j^* / (\bar{N}_j)_{bound}$ given in Fig. 6-1, and from the fact that $\bar{L}^*$ and $(\bar{N})_{bound}$ are each derived from L_j^* and $(\bar{N}_j)_{bound}$, in Eqs.(D.30) and (C.26) respectively, by means of identical averaging operations.

The essential characteristic here is that $\bar{L}^*$ and $\bar{N}$ are of comparable magnitudes. Such a result is, of course, to be expected; when the mean of a sum of statistically independent random variables is already large, the probability in a particular experiment that this average result is exceeded by a large percentage is small. Hesitation with respect to inferring too much about $\bar{L}$, on the basis of $\bar{L}^*$, stems from recognition that the members of the convolutional code set are not, in fact, statistically independent of each other.

It is mentioned in Chapter VI that the average value of the estimated cut-off levels, $\bar{L}^*$, need grow no faster than the square

of the code length n_f. Since this result is derived from a gross bound on $\bar{N}$, we expect that the actual growth is more nearly linear with n_f.

The Decoding Computer. The convolutional encoding technique is characterized by the fact that only a single check digit generator sequence, n_f digits long, need be stored in the computer memory. Every possible transmitted message of length n_f can then be generated, one after the other.

Advantage of this capability is taken in the decoding procedure: The receiving computer is prepared, if necessary, to generate each possible message in turn. The total number of requisite operations is restricted by means of recognizing at small digit-lengths that most of the incorrect messages are thoroughly inconsistent with the received sequence, and discarding them as the decoding process progresses.

In order to accomplish this, the computer need store as a minimum only the generator sequence, the received message, and that particular possible sequence with which it is immediately concerned. The size of the required decoding computer therefore certainly need grow only linearly with increasing convolutional constraint length n_f.

As a practical matter, the decoding procedure can be facilitated by storing in addition whichever message has previously been found to differ from the received sequence in the fewest digits. Then, in the next sequential decoding operation, the computer can start its search for a probable message on the basis of this prior discovery. A procedure of this type should be considerably more

efficient, and no more difficult to program, than one involving straight numerical progression.

The decoding rules specified in Chapters IV and VI involve a flexible approach, whereby the computer is prepared to spend as much time as may be necessary in order to reach a sound decoding decision. The bounds on the number of decoding computations concern only the ensemble average behavior. We must expect that in practice there will be considerable excursions around the mean. Since data pour into the computer at a fixed rate, and out at a variable rate, it is necessary to provide storage for more than just n_f digits of the received message. However, storage beyond this limit need not be immediately accessible to the computer, since only the next n_f undecoded digits enter into the decoding process. The rest may be placed into "dead" storage on paper or magnetic tape.

In order to lessen waiting-line problems, the speed of the decoding computer must exceed the average demands placed upon it. For communication speeds in the vicinity of 100 teletype words per minute, modern microsecond computer speeds should suffice. Even so, however, the waiting-line problem is considerable. Bad decoding situations occur with a probability that is exponentially small — but when they do occur, they are of exponential magnitude.

In a complete, two-way communications system, this problem can be ameliorated as follows. The important characteristic is that the decoding computer will usually start to labor long before it makes an error. When a particularly unlikely channel error pattern

occurs, undecoded traffic will start to build up. The computer can recognize this, and request over the reverse channel that the transmitter reduce the rate of transmission, R_t. Since the average number of decoding computations is an extraordinarily sensitive function of R_t, the lag of the receiver should soon be overcome, without either retransmission or error.

This same technique can be applied when the channel transition probability p_o is a very slowly varying function of time. In the determination of the important parameter $B = \frac{CR_t/E_m}{C - R_t}$, a decrease in the channel capacity C is approximately equivalent to an increase in R_t. Accordingly, it should be possible to track the variations in the capacity of the channel, and to operate (again without error or retransmission) at the limit of ability of the decoding equipment. On the rare occasions when an error is made, the receiver will, with almost unit probability, recognize the event. In this case, resynchronization of the computers, and retransmission of lost data, are necessary.

In practice, the actual selection of an appropriate convolutional generator sequence g should prove no problem. There are 2^{n_f} possible choices in all, and most of these should be suitable. Care must, of course, be taken to avoid sequences that are obviously poor, such as those exhibiting readily apparent periodicities or marked discrepancies between the number of 0's and 1's.

2. Suggestions for Future Work

It is felt that the theoretical results of this investigation are sufficiently cogent to justify an experimental study. Although for really small probabilities of error it would be difficult to

obtain positive numerical verification of decoding error frequencies by means of Monte Carlo techniques, negative results would still be of interest.

The sequential decoding behavior of the correct message subset should be studied both experimentally and theoretically. The theoretical problem is a difficult one, however. Aside from the question of statistical interdependencies, it would appear almost impossible to incorporate into a mathematical analysis the advantages that accrue through retention of the most probable message discovered during the preceding decoding cycle.

One of the significant results of sequential decoding is the indication that near-optimum procedures exist, which do not imply an exponentially increasing number of computations. It is hoped that with further research other, better, procedures will be forthcoming.

A second significant feature is that the sequential decoding technique essentially involves only the measurement of a posteriori probabilities. On account of this, it should be possible to extend the work reported here in connection with the BSC to the case of more general (and more nearly physical) communication channels.

Appendix A: PROBABILITIES

1. Chernov Bound

In analyzing the behavior of codes, we must often consider the probability of very unlikely events. Since the central-limit theorem gives good estimates only for probabilities near the mean, a different technique must be used to evaluate probabilities lying far out on the tail of a distribution. Following a method of Chernov[13] and Cramer,[14] Shannon[3] has compounded a general procedure for treating this problem. Those of Shannon's results that pertain to the Binary Symmetric Channel are reproduced below.

Let w be a discrete random variable, and dF(w) be its density distribution function. The distribution function F(w) is then given by

$$F(w) = \int_{-\infty}^{w} dF(w) \tag{A.1}$$

The moment generating function f(h) for F(w) is defined in the usual way as

$$f(h) = \int_{-\infty}^{\infty} e^{hw}\, dF(w) \tag{A.2}$$

where F(w) is assumed to have only a finite number of jumps.

In addition to F(w), it is convenient to define a different but related distribution function G(w).

$$G(w) = \frac{\int_{-\infty}^{w} e^{h_1 w} dF(w)}{\int_{-\infty}^{\infty} e^{h_1 w} dF(w)} \tag{A.3}$$

In Eq.(A.3), the normalizing integral in the denominator is just

$f(h_1)$, where h_1 is an arbitrary and as yet unspecified parameter. From Eq.(A.3) it follows by differentiation that

$$dG(w) = \frac{e^{h_1 w} dF(w)}{f(h_1)} \tag{A.4}$$

Now let $g(h)$ be the moment generating function associated with $G(w)$. Then,

$$g(h) = \int_{-\infty}^{\infty} e^{hw} dG(w) = \frac{f(h + h_1)}{f(h_1)} \tag{A.5}$$

We are interested in evaluating the n-fold distribution function $F_n(z)$, where z is the sum of n statistically independent random variables w_i, each of which has the same distribution function $F(w)$. Since moment generating functions multiply when independent random variables add, $F_n(w)$ corresponds to the moment generating function

$$f_n(h) = \left[f(h)\right]^n \tag{A.6}$$

If the $G(w)$ distribution is used instead of $F(w)$, then the n-fold moment generating function is

$$g_n(h) = \frac{f_n(h + h_1)}{\left[f(h_1)\right]^n} \tag{A.7}$$

Equation (A.7) can be written in terms of the defining integrals.

$$\int_{-\infty}^{\infty} e^{hz}\, dG_n(z) = \frac{1}{\left[f(h_1)\right]^n} \int_{-\infty}^{\infty} e^{(h + h_1)z} dF_n(z) \tag{A.8}$$

On account of the monotonic and measurable properties of distribution functions, this equation implies that

$$e^{hz}\, dG_n(z) = \left[f(h_1)\right]^{-n} e^{(h + h_1)z}\, dF_n(z) \tag{A.9}$$

For convenience, now define the semi-invariant generating function, u(h).

$$u(h) = \log_e f(h) \tag{A.10}$$

We can then write Eq.(A.9) in the forms

$$dF_n(z) = e^{nu(h_1)-h_1 z}\, dG_n(z) \tag{A.11}$$

and

$$F_n(z) = e^{nu(h_1)} \int_{-\infty}^{z} e^{-h_1 z}\, dG_n(z) \tag{A.12}$$

Since $F_n(z)$ is a distribution function, its value at infinity is unity.

$$1 = e^{nu(h_1)} \int_{-\infty}^{\infty} e^{-h_1 z}\, dG_n(z) \tag{A.13}$$

Subtracting Eqs.(A.12) and (A.13), we obtain

$$1 - F_n(z) = e^{nu(h_1)} \int_{z}^{\infty} e^{-h_1 z}\, dG_n(z) \tag{A.14}$$

When h_1 is greater than zero, the maximum value of $e^{-h_1 z}$ over the range of integration occurs at the lower limit. If this factor is removed from under the integration sign, and the remaining integral bounded by unity, the following important inequality results.

$$1 - F_n(z) \leqslant e^{nu(h_1)-h_1 z} \qquad (\text{for } h_1 > 0) \tag{A.15}$$

Except for the fact that it must be positive, the parameter h_1 in Eq.(A.15) is as yet completely arbitrary. It is possible to choose h_1 so as to minimize the right-hand side of the inequality. Letting $u'(h_1)$ mean $\frac{d}{dh_1} u(h_1)$, set

$$\frac{d}{dh_1}\left[nu(h_1) - h_1 z\right] = nu'(h_1) - z = 0 \qquad (A.16)$$

Substitution of the value of z determined above into Eq.(A.15), and elimination of the no-longer-required subscript to h, leads to Shannon's result that

$$1 - F_n\left[nu'(h)\right] \leqslant e^{n\left[u(h)-hu'(h)\right]} \quad (\text{for } h>0) \qquad (A.17)$$

Equation (A.17) can be specialized for the Binary Symmetric Channel. Let w=0 be the event "transmitted and received digits agree," and w=1 be the event "transmitted and received digits disagree." Let the channel transition probability be p_o, and $q_o = 1-p_o$.

$$P(w = 1) = p_o \qquad (A.18)$$

$$P(w = 0) = 1 - p_o = q_o \qquad (A.19)$$

Then

$$dF(w) = q_o\,\delta(w) + p_o\,\delta(w-1) \qquad (A.20)$$

where δ is the Dirac impulse function. Accordingly,

$$f(h) = \int_{-\infty}^{\infty} e^{hw}\,dF(w) = q_o + p_o e^h \qquad (A.21)$$

$$u(h) = \log_e f(h) = \log_e(q_o + p_o e^h) \qquad (A.22)$$

and

$$u'(h) = \frac{d\left[u(h)\right]}{dh} = \frac{p_o e^h}{q_o + p_o e^h} \qquad (A.23)$$

We desire to find an expression for the probability that the transmitted and received sequences differ from each other in more than np digits out of a total of n digits. Let d_o be the actual

number of digit errors introduced by the channel.

$$d_o = \sum_{j=1}^{n} w_j \tag{A.24}$$

By definition of the distribution function,

$$P(d_o > np) = 1 - F_n(np) \tag{A.25}$$

In order to apply Eq.(A.17), we must therefore equate np to nu'(h) and solve for h and u(h).

$$p = \frac{p_o e^h}{q_o + p_o e^h} \tag{A.26}$$

$$e^h = \frac{pq_o}{p_o q} \qquad \text{where } q = 1 - p \tag{A.27}$$

$$h = \log_e \frac{pq_o}{p_o q} \qquad \text{where } h>0 \text{ for } p>p_o \tag{A.28}$$

$$u(h) = \log_e\left(q_o + \frac{pq_o}{q}\right)$$

Substituting these values into Eqs.(A.17) and (A.25), we obtain

$$P(d_o > np) \leqslant e^{n\left[\log_e\left(q_o + \frac{pq_o}{q}\right) - p \log_e \frac{pq_o}{p_o q}\right]} \tag{A.29}$$

(for $p>p_o$)

After algebraic manipulation, Eq.(A.29) can be rewritten in terms of entropy functions. When the logarithms are taken to the base 2 instead of to the base e, the final result is

$$P(d_o > np) \leqslant 2^{-n\left[H(p_o) - H(p) + (p-p_o)\log \frac{q_o}{p_o}\right]} \tag{A.30}$$

(for $p>p_o$)

This is the bound on the tail terms of a binomial distribution for which we have been looking.

By similar arguments, starting with Eq.(A.12) and considering the case where h_1 is less than zero, we can obtain the result that

$$P(d_o \leqslant np) \leqslant 2^{-n\left[H(p_o)-H(p)-(p-p_o)\log \frac{q_o}{p_o}\right]} \qquad (\text{for } p<p_o) \qquad (A.31)$$

Of particular interest is the case where two sequences, independently selected at random from the set of all 2^n possible binary sequences of length n, are compared against each other. For this situation, p_o goes into 1/2, and the number of digits in which the two sequences actually differ may be called d_i instead of d_o. Since $H(1/2) = 1$ and $\log(1) = 0$, Eq.(A.31) becomes

$$P(d_i \leqslant np) \leqslant 2^{-n\left[1-H(p)\right]} \qquad (\text{for } p<1/2) \qquad (A.32)$$

2. Block Coding

In block coding, the transmitter and receiver are assumed to have available duplicate copies of a code book S, consisting of an ordered array of $|S|$ message sequences each of which is n_f digits long. The receiver compares the received message with each of the $|S|$ possible transmitter messages, and decides that the one actually transmitted is that which differs from the received sequence by the smallest "distance" - that is, in the smallest number of digits.

Elias[4] has analyzed the probability of error behavior for such codes in considerable detail. For convenience, his results and their derivation (with a few slight modifications) are outlined in the following paragraphs.

Random Block Coding. Assume that the $|S|$ messages in the code book are selected independently at random from the set of all 2^{n_f} binary sequences of length n_f. The rate of transmission R_t, and a corresponding probability parameter p_t, are defined in terms of $|S|$ and n_f by Eq.(A.33) below.

$$|S| = 2^{n_f R_t} = 2^{n_f\left[1-H(p_t)\right]} \qquad (\text{for } p_t < \tfrac{1}{2}) \qquad (A.33)$$

$H(p)$ is the entropy function, taken to the base 2.

The message is decoded correctly if no other sequence in the code book set S differs from the received sequence in fewer digits than does the message actually transmitted. The probability that this condition is not satisfied is the probability of error, P(e). Evaluation of P(e) for a particular code book set S would require complete specification of each of the selected message sequences. We can, however, calculate the average probability of error over the ensemble of all possible sets S: that is, the average value of P(e) when the sequences in S are chosen at random. Call this average value $P(e)_{random}$. Then, summing over the positive integers k,

$$P(e)_{random} = \sum_{k=o}^{n_f} P(d_o = k)\ P(\text{any } d_i \leqslant k) \qquad (A.34)$$

where, as before, d_o is the distance between the received and transmitted sequences, and d_i is the distance between the received and the i^{th} incorrect sequence.

For a BSC with a transition probability p_o,

$$P(d_o = k) = p_o^k\ q_o^{n_f-k} \binom{n_f}{k} \qquad (A.35)$$

Also, when the sequences in S are selected at random,

$$P(d_i \leqslant k) = 2^{-n_f} \sum_{j=o}^{k} \binom{n_f}{j} \tag{A.36}$$

The notation $\binom{n_f}{k}$ indicates the binomial coefficient.

$$\binom{n_f}{k} = \frac{n_f!}{k!(n-k)!} \tag{A.37}$$

There is a total of $|S| - 1$ possible incorrect messages. The probability that any of them lies at a distance less than or equal to k from the received message is

$$P(\text{any } d_i \leqslant k) = 1 - \left[1 - P(d_i \leqslant k)\right]^{|S|-1} \tag{A.38}$$

Therefore,

$$\begin{aligned} P(\text{any } d_i \leqslant k) &< |S|\ P(d_i \leqslant k) && (\text{for r.h.s.} \leqslant 1) \\ &\leqslant 1 && (\text{otherwise}) \end{aligned} \tag{A.39}$$

In writing Eq.(A.38), we make use of the statistical independence between sequences in S. Using Eqs.(A.32) and (A.33), and letting $k_t = np_t$, we obtain the result that

$$\begin{aligned} |S|\ P(d_i \leqslant k) &\leqslant 2^{-n_f\left[H(p_t)-H(k/n_f)\right]} && (\text{for } k/n_f < \tfrac{1}{2}) \\ &\leqslant 1 && (\text{for } k \leqslant k_t < \tfrac{1}{2} n_f) \end{aligned} \tag{A.40}$$

Now we can substitute Eqs.(A.35) and (A.39) into Eq.(A.34), and break the sum at k_t, to obtain the inequality

$$\begin{aligned} P(e)_{\text{random}} < 2^{-n_f} |S| \Bigg[&\sum_{k=o}^{k_t} p_o^k\, q_o^{n_f-k} \binom{n_f}{k} \sum_{j=o}^{k} \binom{n_f}{j} \\ &+ \sum_{k=k_t+1}^{n_f} p_o^k\, q_o^{n_f-k} \binom{n_f}{k} \Bigg] \end{aligned} \tag{A.41}$$

First we evaluate the second summation in Eq.(A.41). In order to obtain a small probability of error, the rate of transmission $R_t = 1 - H(p_t)$ must be smaller than the channel capacity C. Since for the Binary Symmetric Channel, $C = 1 - H(p_o)$, we require that $p_t > p_o$. Then the terms in the second summation decrease monotonically, and the first term may be factored out.

$$\sum_{k=k_t+1}^{n_f} = p_o^{k_t+1} q_o^{n_f-k_t-1} \binom{n_f}{k_t+1} \left[1 + \frac{p_o}{q_o} \cdot \frac{(n_f - k_t - 1)}{(k_t + 2)} + \ldots \right]$$

Let $q_t = 1 - p_t$, and define $r_1 = p_o q_t / q_o p_t$. We replace the summation terms by a geometric series, and obtain the bound

$$\sum_{k=k_t+1}^{n_f} < p_o^{n_f p_t} q_o^{n_f q_t} \binom{n_f}{n_f p_t} \frac{r_1}{1 - r_1}$$

This expression can be evaluated through the use of Stirling's approximation.

$$\sqrt{2\pi m} \left(\frac{m}{e}\right)^m e^{\left(\frac{1}{12m} - \frac{1}{360m^3}\right)} < m! < \sqrt{2\pi m} \left(\frac{m}{e}\right)^m e^{1/12m}$$

From these bounds on m!, it is possible to obtain corresponding bounds on the binomial coefficient. For $q = 1 - p$,

$$\frac{1}{\sqrt{8npq}} 2^{mH(p)} < \binom{m}{mp} < \frac{1}{\sqrt{2\pi m\, pq}} 2^{mH(p)} \quad \text{(for } p \neq 0,1\text{)} \qquad \text{(A.42)}$$

A certain amount of algebraic manipulation then leads to the result that

$$\sum_{k=k_t+1}^{n_f} < \frac{p_o q_t}{(p_t - p_o)} \cdot \frac{1}{\sqrt{2\pi n_f p_t q_t}} 2^{-n_f \left[H(p_o) - H(p_t) + (p_t - p_o) \log \frac{q_o}{p_o} \right]} \quad \text{(for } p_o < p_t < \tfrac{1}{2}\text{)} \qquad \text{(A.43)}$$

Evaluation of the first summation of Eq.(A.41) is somewhat more complicated. Since $k \leqslant k_t < \frac{1}{2} n_f$, it follows that the interior summation on j can also be bounded by a geometric series.

$$\sum_{j=o}^{k} \binom{n_f}{j} < \binom{n_f}{k} \frac{1}{1 - r_2} \quad , \quad \text{where } r_2 = \frac{k}{n_f - k}$$

The largest value of r_2 occurs for $k = k_t = n_f p_t$. Therefore,

$$\sum_{k=o}^{k_t} < \frac{1}{1 - \frac{p_t}{q_t}} \sum_{k=o}^{k_t} p_o^{\,k} q_o^{\,n_f - k} \binom{n_f}{k}^2 \qquad (A.44)$$

The last term may be factored out of the remaining summation on k.

$$\sum_{k=o}^{k_t} < \frac{1}{1 - \frac{p_t}{q_t}} p_o^{\,k_t} q_o^{\,n_f - k_t} \binom{n_f}{k_t}^2 \left[1 + \frac{q_o}{p_o} \cdot \left(\frac{k_t}{n_f - k_t + 1} \right)^2 + \ldots \right] \qquad (A.45)$$

Define $q_{crit} = 1 - p_{crit}$, and

$$\frac{p_{crit}}{q_{crit}} = \sqrt{\frac{p_o}{q_o}} \qquad (A.46)$$

If $p_t < p_{crit}$, then the summation is again dominated by a geometric series.

$$\sum_{k=o}^{k_t} < \frac{1}{1 - \frac{p_t}{q_t}} \cdot \frac{1}{1 - \frac{q_o}{p_o}\left(\frac{p_t}{q_t}\right)^2} p_o^{\,k_t} q_o^{\,n_f - k_t} \binom{n_f}{k_t}^2 \quad (\text{for } p_t < p_{crit})$$

Algebraic manipulation, use of Stirling's approximation, and substitution of Eq.(A.33) lead finally to the result that

$$|S|\, 2^{-n_f} \sum_{k=o}^{k_t} < \frac{1}{\left(1 - \frac{p_t}{q_t}\right)\left[1 - \frac{q_o}{p_o}\left(\frac{p_t}{q_t}\right)^2\right]} \cdot \frac{2^{-n_f\left[H(p_o)-H(p_t)+(p_t-p_o)\log \frac{q_o}{p_o}\right]}}{2\pi n_f\, p_t q_t}$$

$$(\text{for } p_o < p_t < p_{crit}) \qquad (A.47)$$

When $p_t \geqslant p_{crit}$, the largest term in the summation of Eq.(A.44) is that for which $k = n_f p_{crit}$. The summation can then be bounded by the number of terms ($k_t = n_f p_t$) multiplied by the largest term.

$$\sum_{k=o}^{k_t} < \frac{k_t}{1 - \frac{p_t}{q_t}}\, p_o^{\,n_f p_{crit}}\, q_o^{\,n_f q_{crit}} \binom{n_f}{n_f p_{crit}}^2 \quad (\text{for } p_{crit} \leqslant p_t < \tfrac{1}{2})$$

For this situation, we obtain the bound

$$|S|\, 2^{-n_f} \sum_{k=o}^{k_t} < \frac{1}{1 - \frac{p_t}{q_t}} \cdot \frac{p_t}{2\pi p_{crit} q_{crit}} \cdot$$

$$\cdot\; 2^{-n_f\left[H(p_o)-H(p_{crit})+(p_{crit}-p_o)\log \frac{q_o}{p_o}+H(p_t)-H(p_{crit})\right]}$$

$$(\text{for } p_{crit} \leqslant p_t < \tfrac{1}{2}) \qquad (A.48)$$

Equations (A.43), (A.46), and (A.47) can now be substituted into the expression for the probability of error, Eq.(A.41). The results are summarized below. The channel transition probability is p_o, and the rate of transmission R_t and its associated probability parameter p_t are determined by the code book set S and the block length n_f.

$$|S| = 2^{n_f R_t} = 2^{n_f\left[1-H(p_t)\right]} \qquad (\text{for } p_t < \tfrac{1}{2}) \qquad (A.33)$$

Also,

$$\frac{p_{crit}}{q_{crit}} = \sqrt{\frac{p_o}{q_o}} \tag{A.46}$$

Now let

$$A_r = \frac{1}{\left(1 - \frac{p_t}{q_t}\right)\left[1 - \frac{q_o}{p_o}\left(\frac{p_t}{q_t}\right)^2\right]} \cdot \frac{1}{2\pi n_f p_t q_t} \tag{A.49}$$

$$A_t = \frac{1}{\sqrt{2\pi n_f p_t q_t}} \cdot \frac{p_o q_t}{(p_t - p_o)} \tag{A.50}$$

$$A_{crit} = \frac{1}{\left(1 - \frac{p_t}{q_t}\right)} \cdot \frac{p_t}{2\pi p_{crit} q_{crit}} \tag{A.51}$$

$$E_t = H(p_o) - H(p_t) + (p_t - p_o) \log \frac{q_o}{p_o} \tag{A.52}$$

$$E_{crit} = H(p_o) - H(p_{crit}) + (p_{crit} - p_o) \log \frac{q_o}{p_o} + H(p_t) - H(p_{crit}) \tag{A.53}$$

Then

$$P(e)_{random} < (A_r + A_t)\, 2^{-n_f E_t} \qquad (\text{for } p_o < p_t < p_{crit}) \tag{A.54}$$

$$P(e)_{random} < A_{crit}\, 2^{-n_f E_{crit}} + A_t\, 2^{-n_f E_t} \qquad (\text{for } p_{crit} \leqslant p_t < \tfrac{1}{2}) \tag{A.55}$$

Optimum Block Coding. Consider now another code book of $|S|_{opt}$ possible message sequences, each of which is also n_f digits long. Assume that it were possible to choose these messages so that all sets of $k_1 < \frac{1}{2} n_f$ or fewer transmission errors could be corrected. This implies that the decoder associates with each message

that subset of all binary sequences of length n_f which differ from it in k_1 or fewer digits. It also implies that all of these $|S|_{opt}$ subsets are disjoint. Since there are altogether only 2^{n_f} different binary sequences of length n_f, it follows that

$$|S|_{opt} \leqslant \frac{2^{n_f}}{\sum_{k=0}^{k_1} \binom{n_f}{k}} < \frac{2^{n_f}}{\binom{n_f}{k_1}} \tag{A.56}$$

Using Stirling's approximation, we obtain the bound

$$|S|_{opt} < \sqrt{8n_f p_1 q_1}\ 2^{n_f\left[1-H(p_1)\right]} \tag{A.57}$$

and hence

$$R_t = \frac{1}{n_f} \log |S|_{opt} < 1 - H(p_1) + \frac{1}{2n_f} \log 8n_f p_1 q_1 \tag{A.58}$$

where $k_1 = n_f p_1$ and $q_1 = 1 - p_1$.

The probability of error is just the probability that more than k_1 transmission errors occur.

$$P(e)_{opt} = \sum_{k=k_1+1}^{n_f} p_o^{\,k}\, q_o^{\,n_f-k} \binom{n_f}{k} \tag{A.59}$$

Although in general we do not actually know how to construct the code book set S_{opt} in the implied fashion, it is certain that no other choice of $|S|_{opt}$ sequences could result in a lower probability of error than $P(e)_{opt}$, since changing any sequence from one decoding subset to another can only increase this probability.

For $p_1 > p_o$, the first term of the summation in Eq.(A.59) is greatest.

$$P(e)_{opt} > p_o^{k_1+1} q_o^{n_f-k_1-1} \binom{n_f}{k_1+1}$$

Use of Stirling's approximation then leads to the bound

$$P(e)_{opt} > \frac{1}{\sqrt{8n_f p_1 q_1}} \cdot \frac{p_o q_1}{q_o\left(p_1 + \frac{1}{n_f}\right)} \; 2^{-n_f\left[H(p_o)-H(p_1)+(p_1-p_o)\log \frac{q_o}{p_o}\right]} \quad (\text{for } p_o < p_1 < \tfrac{1}{2}) \tag{A.60}$$

In the limit as n_f approaches infinity, Eqs.(A.58) and (A.60) go into the asymptotic relations

$$R_t \lesssim 1 - H(p_1) \tag{A.61}$$

and

$$P(e)_{opt} \gtrsim A_{opt} \; 2^{-n_f E_1} \quad (\text{for } p_o < p_1 < \tfrac{1}{2}) \tag{A.62}$$

where

$$A_{opt} = \frac{p_o q_1}{q_o p_1} \cdot \frac{1}{\sqrt{8n_f p_1 q_1}} \tag{A.63}$$

and

$$E_1 = H(p_o) - H(p_1) + (p_1 - p_o) \log \frac{q_o}{p_o} \tag{A.64}$$

Comparison of these results with those for random block coding shows that in the limit of large block length n_f, random coding is exponentially equivalent to the optimum block code for rates of transmission R_t greater than R_{crit}, where

$$R_{crit} = 1 - H(p_{crit}) \tag{A.65}$$

Thus, for small probabilities of error - which implies large block length - the average probability of error over the ensemble of all possible block codes is at least exponentially as good as that obtained with the best possible such code, when $R_t < R_{crit}$.

Appendix B: APPROXIMATIONS

1. Approximation to H(p)

The entropy function H(p), taken to the base 2, is defined as

$$H(p) = - p \log p - q \log q \tag{B.1}$$

where $q = 1 - p$. In order to simplify mathematical analysis, it is sometimes convenient to replace the transcendental function H(p) with an algebraic function $H_1(p)$, chosen to provide an approximation to H(p) over a range of p from $0 \leqslant p_a \leqslant p \leqslant p_b \leqslant \frac{1}{2}$. A suitable function $H_1(p)$ may be written in the form below.

$$H_1(p) = A_o + A_1\sqrt{1 + A_2(p - p_a)} - A_3(p - p_a) \tag{B.2}$$

The coefficients A_i are evaluated by equating $H_1(p)$ to H(p), and $H_1'(p)$ to H'(p), at the end-points p_a and p_b. The prime notation means differentiation with respect to the argument.

$$\left.\begin{aligned} H_1(p_a) &= H(p_a) & H_1'(p_a) &= H'(p_a) \\ H_1(p_b) &= H(p_b) & H_1'(p_b) &= H'(p_b) \end{aligned}\right\} \tag{B.3}$$

Since both $H_1(p)$ and H(p) are smooth and continuous functions with monotonically decreasing first derivatives, the maximum difference between $H_1(p)$ and H(p) decreases as $(p_b - p_a)$ is reduced, when Eqs.(B.3) are satisfied. By dividing a larger range of p into enough subintervals, a smooth and continuous piecewise approximation to H(p) can be made to any desired degree of accuracy.

2. Upper Bound to H(p)

We are particularly interested in $H_1(p)$ when $p_a = p_o$ (the BSC transition probability) and $p_b = \frac{1}{2}$. Under these conditions

Eqs.(B.3) become

$$\left.\begin{aligned} A_o + A_1 &= H(p_o) \\ A_o + A_1\sqrt{1 + A_2\left(\tfrac{1}{2} - p_o\right)} - A_3\left(\tfrac{1}{2} - p_o\right) &= 1 \\ \tfrac{1}{2} A_1 A_2 - A_3 &= \log \frac{q_o}{p_o} \\ \frac{\tfrac{1}{2} A_1 A_2}{\sqrt{1 + A_2\left(\tfrac{1}{2} - p_o\right)}} - A_3 &= 0 \end{aligned}\right\} \qquad (B.4)$$

Define

$$E_m = \left(\tfrac{1}{2} - p_o\right) \log \frac{q_o}{p_o} - C \qquad (B.5)$$

where C is the channel capacity.

$$C = 1 - H(p_o) \qquad (B.6)$$

Then the solutions to Eqs.(B.4) are

$$\left.\begin{aligned} A_o &= H(p_o) - \frac{2C^2 E_m}{(E_m - C)^2} \\ A_1 &= \frac{2C^2 E_m}{(E_m - C)^2} \\ A_2 &= \frac{E_m - C}{C^2} \log \frac{q_o}{p_o} \\ A_3 &= \frac{C}{E_m - C} \log \frac{q_o}{p_o} \end{aligned}\right\} \qquad (B.7)$$

When these values for A_i are substituted into Eq.(B.2), we obtain finally

$$H_1(p) = H(p_o) - \frac{2C^2E_m}{(E_m - C)^2} + \frac{2C^2E_m}{(E_m - C)^2}\sqrt{1 + \frac{E_m - C}{C^2}\left(\log \frac{q_o}{p_o}\right)(p - p_o)}$$

$$- \frac{C}{E_m - C}\left(\log \frac{q_o}{p_o}\right)(p - p_o) \qquad (B.8)$$

It can be shown that $H_1(p)$, as given by Eq.(B.8), is not only an approximation but also an upper bound to $H(p)$. That is, that

$$H_1(p) \geqslant H(p) \qquad (\text{for } p_o \leqslant p \leqslant \tfrac{1}{2}) \qquad (B.9)$$

This important result follows from consideration of the second derivatives of $H_1(p)$ and $H(p)$.

$$H_1''(p) = \frac{-\frac{E_m}{2C^2}\left(\log \frac{q_o}{p_o}\right)^2}{\left[1 + \frac{E_m - C}{C^2}\left(\log \frac{q_o}{p_o}\right)(p - p_o)\right]^{3/2}} \qquad (B.10)$$

$$H''(p) = -\frac{\log e}{pq} \qquad (B.11)$$

Hypothesize for the moment that

$$\left.\begin{aligned} H_1''(p_o) &= -\frac{1}{2}\frac{E_m}{C^2}\left(\log \frac{q_o}{p_o}\right)^2 > H''(p_o) = \frac{-\log e}{p_o q_o} \\ H_1''\left(\tfrac{1}{2}\right) &= -\frac{1}{2}\frac{C}{E_m^2}\left(\log \frac{q_o}{p_o}\right)^2 > H''\left(\tfrac{1}{2}\right) = -4 \log e \end{aligned}\right\} \qquad (B.12)$$

Now define the function

$$f(p) = H_1(p) - H(p) \qquad (B.13)$$

We have adjusted the coefficients in Eq.(B.8) so that

$$f(p) = 0 \qquad (\text{at } p = p_o \text{ and } p = \tfrac{1}{2}) \qquad (B.14)$$

and

$$f'(p) = 0 \qquad (\text{at } p = p_o \text{ and } p = \tfrac{1}{2}) \tag{B.15}$$

By the hypothesis of Eq.(B.12),

$$f''(p) = H_1''(p) - H''(p) > 0 \qquad (\text{at } p = p_o \text{ and } p = \tfrac{1}{2}) \tag{B.16}$$

and therefore $H_1(p) \geqslant H(p)$ near the end-points of the closed interval $(p_o, \frac{1}{2})$.

We also know by the Theorem of the Mean that the equation

$$f'(p) = 0 \tag{B.17}$$

must have at least one solution at a point interior to the interval. By the same token, the equation

$$f''(p) = 0 \tag{B.18}$$

must have at least two interior solutions. If $f''(p) = 0$ has two and only two solutions, then $f'(p)$ can equal zero at only one interior point, and $H_1(p)$ is consequently greater than $H(p)$ for all points p such that $p_o \leqslant p \leqslant \frac{1}{2}$.

Define

$$g(p) = \left[H_1''(p)\right]^2 - \left[H''(p)\right]^2 \tag{B.19}$$

Whenever $f''(p) = 0$,

$$g(p) = 0 \tag{B.20}$$

Substituting Eqs.(B.10) and (B.11) into Eq.(B.19), we have

$$g(p) = \frac{\dfrac{E_m^2}{4C^4}\left(\log \dfrac{q_o}{p_o}\right)^4 p^2(1-p)^2 - \left[1 + \dfrac{E_m - C}{C^2}\left(\log \dfrac{q_o}{p_o}\right)(p - p_o)\right]^3 (\log e)^2}{\left[1 + \dfrac{E_m - C}{C^2}\left(\log \dfrac{q_o}{p_o}\right)(p - p_o)\right]^3 p^2(1-p)^2} \tag{B.21}$$

The cubic factor in the denominator of $g(p)$ varies from 1 at $p = p_o$ to $\left(\frac{E_m}{C}\right)^3$ at $p = \frac{1}{2}$, and is always positive in between. The numerator of $g(p)$ is quartic, and p^4 has a positive coefficient. The numerator therefore approaches plus infinity as p approaches either plus or minus infinity.

On the other hand, by the hypothesis of Eq.(B.12), $g(p)$ is negative for both $p = p_o$ and $p = \frac{1}{2}$. It follows that the numerator of $g(p)$ must have two roots outside the interval $\left(p_o, \frac{1}{2}\right)$, and accordingly $g(p)$ must have exactly two roots within the interval. Subject only to verification of Eqs.(B.12), we have proved the validity of Eq.(B.9).

In Table A.1 are compiled values of $H_1''(p_o)$, $H''(p_o)$, $H_1''\left(\frac{1}{2}\right)$, and $H''\left(\frac{1}{2}\right)$ for various representative values of p_o.

TABLE A.1

p_o	$H_1''(p_o)$	$H''(p_o)$	$H_1''\left(\frac{1}{2}\right)$	$H''\left(\frac{1}{2}\right)$
.450	- 5.82	- 5.84	- 5.76	- 5.78
.400	- 5.98	- 6.01	- 5.73	- 5.78
.100	- 13.13	- 16.05	- 4.92	- 5.78
.050	- 21.2	- 30.4	- 4.49	- 5.78
.020	- 39.2	- 73.7	- 4.02	- 5.78
.010	- 60.5	- 145.9	- 3.72	- 5.78
.005	- 90.5	- 290	- 3.49	- 5.78

It is seen that the hypothesis of Eq.(B.12) is in fact true. We conclude that the algebraic approximation given by Eq.(B.8) is an upper bound to the entropy function over the closed interval $\left(p_o, \frac{1}{2}\right)$, for all p_o such that $0 < p_o < \frac{1}{2}$.

3. The Probability Criterion K

In Appendix A, we have derived the following two inequalities:

$$P(d_o > np) \leqslant 2^{-n\left[H(p_o)-H(p)+(p-p_o)\log \frac{q_o}{p_o}\right]} \quad (\text{for } p>p_o) \qquad (A.30)$$

$$P(d_i \leqslant np) \leqslant 2^{-n\left[1-H(p)\right]} \quad (\text{for } p \leqslant \tfrac{1}{2}) \qquad (A.32)$$

For random block coding, d_o is defined as the distance between the received and the transmitted sequence, and d_i is the distance between the received and the i^{th} incorrect sequence in the code book set S.

Now consider a positive number K, and let p_K be the solution to the transcendental equation

$$K = n\left[H(p_o) - H(p_K) + (p_K - p_o)\log \frac{q_o}{p_o}\right] \quad (\text{for } p_K > p_o) \qquad (B.22)$$

If we define

$$k_n = np_K \qquad (B.23)$$

then, by Eq.(A.30),

$$P(d_o > k_n) \leqslant 2^{-K} \quad (\text{for } k_n > np_o) \qquad (B.24)$$

The constant K plays the role of a probability criterion, and k_n is the associated distance criterion. For a given channel transition probability p_o, k_n is completely determined by the probability criterion K and the number of digits n. The distance k_n increases monotonically with both K and n.

With p_K determined by Eq.(B.22), we may define

$$R_K(n) = 1 - H(p_K) \quad (\text{for } p_K \leqslant \tfrac{1}{2}) \qquad (B.25)$$

Then, in accordance with Eq.(A.32), we have the inequality

$$P(d_i \leqslant k_n) \leqslant 2^{-nR_K(n)} \qquad (\text{for } k_n \leqslant \tfrac{1}{2} n) \qquad (B.26)$$

The function $R_K(n)$ has the dimensions of a rate of transmission.

It is instructive to consider the geometric interpretation of p_K and $R_K(n)$, as illustrated in Fig. 4-2 . Given K, for every value of n construct a line segment of length $E_K = \frac{K}{n}$. The slope of the tangent to H(p) at $p = p_o$ is $\log \frac{q_o}{p_o}$. Holding E_K vertical, slide it between the curve H(p) and the tangent line at p_o until it fits exactly. The value of p for which this condition is satisfied is p_K , and $R_K(n)$ is the distance between $H\left(\frac{1}{2}\right)$ and $H(p_K)$.

The maximum permissible value of E_K for which Eq.(B.26) is valid occurs for $p_K = \frac{1}{2}$. This is the value E_m , given in Eq.(B.5). Accordingly, for a given K, we can extend the definition of Eq.(B.26).

$$R_K(n) = 0 \qquad (\text{for } n \leqslant (n_K)_{min} = \tfrac{K}{E_m}) \qquad (B.27)$$

On the other hand, for fixed K, the function $R_K(n)$ approaches the capacity C asymptotically as n approaches infinity. $R_K(n)$ is a monotonic increasing function of n, and a monotonic decreasing function of K.

4. Lower Bound to $R_K(n)$

The equations determining $R_K(n)$ are implicit and transcendental. However, we have already shown that

$$H_1(p) \geqslant H(p) \qquad (\text{for } p_o \leqslant p \leqslant \tfrac{1}{2}) \qquad (B.9)$$

where $H_1(p)$ is the algebraic approximation to H(p) given by Eq.(B.8). If $H_1(p)$ is substituted for H(p) in Eqs.(B.22) and (B.25), then we obtain the bound,

$$R_K(n) \geqslant C - \frac{2C}{\sqrt{E_m}} \sqrt{\frac{K}{n}} + \frac{C}{E_m} \frac{K}{n} \qquad (\text{for } n > (n_K)_{min}) \qquad (B.28)$$

The fact that this is a lower bound to $R_K(n)$ follows directly from Eq.(B.9) and the geometric construction: if $H_1(p) \geqslant H(p)$, then a given line segment E_K will not fit so far to the left in Fig. 4-2.

Direct derivation of Eq.(B.28) is somewhat tedious. It is easier to work backwards, using undetermined coefficients and simplified variables. Let $E_K = \frac{K}{n}$ go into z^2, and $R_K(n)$ go into $R_1(z)$, when $H(p)$ goes into $H_1(p)$. Then Eq.(B.22) becomes

$$z^2 = H(p_o) - H_1(p) + (p - p_o) \log \frac{q_o}{p_o} \qquad (B.29)$$

Assume that $R_1(z)$ has the same form as the r.h.s. of Eq.(B.28),

$$1 - H_1(p) = C - A_4 z + A_5 z^2 \qquad (B.30)$$

If Eqs.(B.29) and (B.30) are to be consistent, then the form which $H_1(p)$ must have is uniquely specified. Substituting Eq.(B.30) into Eq.(B.29), and manipulating, we have

$$z^2(1 - A_5) + A_4 z - (p - p_o) \log \frac{q_o}{p_o} = 0 \qquad (B.31)$$

This quadratic equation relates the variables z and p. Solving,

$$z = \frac{-A_4 + \sqrt{A_4^2 + 4(1 - A_5) \log \frac{q_o}{p_o} (p - p_o)}}{2(1 - A_5)} \qquad (B.32)$$

and

$$z^2 = \frac{A_4^2}{2(1 - A_5)^2} - \frac{A_4}{2(1 - A_5)^2} \sqrt{A_4^2 + 4(1 - A_5) \log \frac{q_o}{p_o} (p - p_o)} + \frac{\log \frac{q_o}{p_o}}{1 - A_5} (p - p_o) \qquad (B.33)$$

This value of z^2 can be substituted back into Eq.(B.29), and the result solved for $H_1(p)$.

$$H_1(p) = \left[H(p_o) - \frac{A_4^2}{2(1-A_5)^2} \right] + \frac{A_4^2}{2(1-A_5)^2} \sqrt{1 + \frac{4(1-A_5)}{A_4^2} \log \frac{q_o}{p_o} (p-p_o)} - \frac{A_5}{1-A_5} \log \frac{q_o}{p_o} (p-p_o) \qquad (B.34)$$

Thus we find that the assumed form of $R_1(z)$ leads independently to an expression for $H_1(p)$ which is of the same form as Eq.(B.8).

When the coefficients of Eqs.(B.34) and (B.8) are equated to each other, we find that

$$A_4 = \frac{2C}{\sqrt{E_m}} \quad ; \quad A_5 = \frac{C}{E_m} \qquad (B.35)$$

It follows from the considerations above that substitution of $H_1(p)$ for $H(p)$ in the determination of $R_K(n)$ yields the result

$$R_1(z) = C - \frac{2C}{\sqrt{E_m}} z + \frac{C}{E_m} z^2 \qquad (B.36)$$

where $z = \sqrt{\frac{K}{n}}$

Moreover, since $H_1(p) \geq H(p)$ for $p_o \leq p \leq \frac{1}{2}$, $R_1(z)$ must be less than or equal to $R_K(n)$ for $n > \frac{K}{E_m}$. The validity of Eq.(B.28) is thus established.

Appendix C: DECODING COMPUTATIONS ON INCORRECT MESSAGES

1. Upper Bound to $\overline{N}_K$

Let us represent by the symbol S the entire set of all possible messages of any given length n, generated by the convolutional process discussed in Chapter III. It is shown in that chapter that, for any n, S forms a group under the operation of sequence addition modulo-2. It is also shown there that, on account of the symmetry properties of groups, we may always assume for purposes of analysis that the transmitted message s_o is the identity sequence of all zeros.

In the proposed decoding process, the objective is to determine, in turn, each of the information digits implied by the received message y. We accomplish this by comparison operations, performed on y and the set of all possible messages, and extending over the length n_f of the convolutional constraints. In accordance with the assumption that s_o is the identity sequence, it is then perfectly general to consider only a truncated message set S_f. We define S_f to be that set of all possible transmitted sequences n_f digits long, which results when every information digit occurring prior to the one currently being decoded is zero.

We now further define S_o to be that subset of all members of S_f whose corresponding information sequence begins with the correct symbol "0". The complementary subset S_1 of "incorrect" messages comprises by elimination all members of S_f whose corresponding information sequence has a "1" in the first digit.

This nomenclature is illustrated in Fig.3-1, for a rate of transmission $R_t = 1/3$ and a prefix length $n_o = 3$. These two quantities, the prefix length and the transmission rate, must always be related by the diophantine constraint

$$n_o R_t = \text{a positive integer} \tag{C.1}$$

Thus, at any length $n = \ell n_o$, where ℓ is a positive integer, the number of different sequences belonging to S_f is exactly

$$\left|S_f(n)\right| = 2^{\ell n_o R_t} = 2^{nR_t} \tag{C.2}$$

It may be seen from Fig.3-1, however, that at length $n = \ell n_o + 1$ the number of possible sequences jumps to

$$\left|S_f(n)\right| = 2^{(\ell+1)n_o R_t} = 2^{(\frac{n-1}{n_o}+1)n_o R_t} \tag{C.3}$$

on account of the tree-structure of the message set. The r.h.s. of Eq.(C.3) forms a bound on $\left|S_f(n)\right|$ for any length n.

$$\left|S_f(n)\right| \leqslant 2^{(n_o-1)R_t} \cdot 2^{nR_t} \tag{C.4}$$

Since exactly one-half of the total number of messages in S_f belong to the incorrect subset S_1, we have finally the inequality

$$\left|S_1(n)\right| \leqslant D_o 2^{nR_t} \tag{C.5}$$

where

$$D_o = \frac{1}{2} 2^{(n_o-1)R_t} \tag{C.6}$$

Next consider any particular sequence s_i in S_1. It is also shown in Chapter III that, as the convolutional generator sequence g takes on all possible values, s_i runs in one-to-one correspondence

through the set of all 2^{n_f} binary numbers of length n_f. Over the ensemble of possible g's, the probability that s_i and the received message agree in any digit is therefore exactly 1/2, and every digit is statistically independent of all others.

This is the same situation discussed in Appendix B. Accordingly, when we average over the ensemble of all possible generator sequences g, we have the probability result that

$$P(d_i \leqslant k_n) \leqslant 2^{-nR_K(n)} \qquad \text{(B.26) and (B.27)}$$

In this equation, d_i is the distance between the received sequence and the i^{th} member of the incorrect subset S_1, k_n equals np_K, and $R_K(n)$ is equal to $1 - H(p_K)$. This result is valid for any particular choice of i, and for any arbitrary choice of the probability criterion K.

There is a total of $\left|S_1(n)\right|$ distinct sequences of length n in the incorrect subset. Also, the average of a sum is equal to the sum of the averages. The ensemble average number of sequences in S_1 that are "probable according to criterion K" — that is, which differ from the received sequence in k_n or fewer digits out of n — is therefore

$$\overline{M}_K(n) = \left|S_1(n)\right| P(d_i \leqslant k_n) \qquad \text{(C.7)}$$

For any given (but unspecified) generator sequence g, and probability criterion K, let us now consider a decoding computer which starts out to generate sequentially the entire subset S_1 of incorrect messages. As it proceeds, however, it discards as improbable every sequence s_i for which d_i becomes greater than k_n.

In order to advance from length n to length (n+1), the computer need never generate more than two additional binary digits for each retained sequence of length n. As a matter of fact, since the number of sequences in S increases only at node points, for many values of n only one additional digit need be computed. Let $\Delta(n)$ equal 2 or 1, depending upon whether or not the tree structure of S has nodes at length n.

We now define a binary computation to be the convolutional generation of a binary digit, plus its comparison against the received message. If no sequences were discarded beforehand, the number of binary computations $N_K(n)$ which the computer would require to progress from length n to length (n+1) would be equal to $\Delta(n)M_K(n)$, where $M_K(n)$ is the number of messages of length n in the complete subset S_1 which are probable according to criterion K. Since discarding messages en route can not increase $N_K(n)$, in the actual operation of the computer we have

$$N_K(n) \leqslant \Delta(n)M_K(n) \qquad (C.8)$$

The total number of binary computations N_K which the computer must make in working progressively through the entire incorrect subset is therefore bounded by the summation of $N_K(n)$ over all lengths n.

$$N_K \leqslant \sum_{n=1}^{n_f} \Delta(n)M_K(n)$$

The equation above is valid for any particular generator sequence g. Next we may average N_K over the ensemble of all g's. The numbers $M_K(n)$ then become random variables, whereas $\Delta(n)$ of

course is still a perfectly definite function of n only. Since the average of a sum is equal to the sum of the averages,

$$\bar{N}_K \leqslant \sum_{n=1}^{n_f} \Delta(n)\bar{M}_K(n) \qquad (C.9)$$

$\bar{N}_K$ is the ensemble average number of binary computations which the decoding computer must make upon the incorrect subset S_1.

The function $\bar{M}_K(n)$ is shown in Eq.(C.7) to be the product of $\left|S_1(n)\right|$ and $P(d_i \leqslant k_n)$. Furthermore, it can be demonstrated* that the over-bound on $\left|S_1(n)\right|$ given by Eq.(C.5) is sufficiently gross that the product of $\Delta(n)$ and $\left|S_1(n)\right|$ is less than or equals $D_o 2^{(n+1)R_t}$, for all values of n. Using this fact, and substituting Eqs.(C.5), (C.6), (C.7), and (B.26) and (B.27) into Eq.(C.9), we have finally

$$\bar{N}_K < D_1 \sum_{n=1}^{n_f} 2^{n\left[R_t - R_K(n)\right]} \qquad (C.10)$$

where

$$D_1 = 2^{(n_o R_t - 1)} \qquad (C.11)$$

It is shown in Appendix B that $R_K(n)$ approaches C as n approaches infinity. For $R_t < C$ and sufficiently large n_f, we therefore expect on the average that the computer will discard every member of the subset S_1.

Rough Bound on N_K. The ensemble average number of binary computations, which a computer must make in the process of discarding the entire incorrect subset S_1 as improbable according to criterion K, is bounded in Eq.(C.10). This inequality is strengthened

---

* See Section 3 of this appendix.

if we substitute a lower bound for $R_K(n)$. From Appendix B,

$$R_K(n) \geqslant C - \frac{2C}{\sqrt{E_m}} \sqrt{\frac{K}{n}} + \frac{C}{E_m} \frac{K}{n} \qquad (B.28)$$

$$(\text{for } n > (n_K)_{min} = \frac{K}{E_m})$$

and

$$R_K(n) = 0 \qquad (\text{for } n \leqslant (n_K)_{min} = \frac{K}{E_m}) \qquad (B.27)$$

For $n < (n_K)_{min}$, all of the branches in the tree-structure of S_i must be generated and retained: the total number of such branches is bounded by $D_o 2^{(n_K)_{min} R_t}$ times a geometric sum, and there are n_o digits in each branch. Accordingly,

$$N_K < \frac{n_o D_o}{1 - 2^{-n_o R_t}} 2^{(n_K)_{min} R_t} + D_1 \sum_{n=(n_K)_{min}}^{n_f} 2^{n\left[R_t - C + \frac{2C}{\sqrt{E_m}} \sqrt{\frac{K}{n}} - \frac{C}{E_m} \frac{K}{n}\right]} \qquad (C.12)$$

The maximum term in the summation above is equal to 2^{KB}, where

$$B = \frac{CR_t/E_m}{C - R_t} \qquad (C.13)$$

The r.h.s. of Eq.(C.12) is bounded by the product of n_f and the largest term. Finally, therefore, we have the rough bound that

$$\bar{N}_K < D_1 n_f 2^{KB} \qquad (C.14)$$

Tight Bound on N_K. When the summand has a single maximum, a summation over unit steps is bounded above by the corresponding integral plus the maximum term. If Eq.(C.12) is evaluated in this way, we obtain a much tighter bound on $\bar{N}_K$.

$$\bar{N}_K < D_1 \left[\frac{n_o 2^{-R_t}}{1 - 2^{-n_o R_t}} 2^{\frac{K}{E_m} R_t} + 2^{KB} \right.$$

$$\left. + \int_{K/E_m}^{n_f} 2^{n(R_t - C) + \frac{2C}{\sqrt{E_m}}\sqrt{Kn} - \frac{C}{E_m}K} \, dn \right] \qquad (C.15)$$

The upper limit of integration can be taken as infinity, which serves to simplify the result without substantially affecting it. The value of the definite integral is found by completing the square.

$$\int_{K/E_m}^{\infty} dn = \frac{2^{KB}}{C - R_t} \left[(\log e)\, 2^{-R_t^2 \left(\frac{K/E_m}{C - R_t} \right)} \right.$$

$$\left. + \frac{2C}{\sqrt{E_m}} \sqrt{\frac{\pi K \log e}{C - R_t}} \operatorname{erf} \left(- R_t \sqrt{\frac{K/E_m}{C - R_t} \cdot \frac{2}{\log e}} \right) \right] \qquad (C.16)$$

where the error function is defined as

$$\operatorname{erf} z = \frac{1}{\sqrt{2\pi}} \int_z^{\infty} e^{-\tau^2/2} \, d\tau \qquad (C.17)$$

The error function, in turn, may be bounded by unity; since its argument in Eq.(C.17) is negative, for large values of K this is a reasonable as well as a conservative approximation. When this bound on the integral is substituted into Eq.(C.15), after algebraic manipulation we obtain the following final result:

$$\bar{N}_K \leqslant D_1 \left[(D_2 + D_3)\, 2^{K \frac{R_t}{E_m}} + (1 + D_4 \sqrt{K}\,)\, 2^{KB} \right] \qquad (C.18)$$

where

$$D_1 = 2^{(n_o R_t - 1)} \tag{C.11}$$

$$D_2 = \frac{n_o 2^{-R_t}}{1 - 2^{-n_o R_t}} \tag{C.19}$$

$$D_3 = \frac{\log e}{C - R_t} \tag{C.20}$$

$$D_4 = \frac{2C}{(C - R_t)^{3/2}} \sqrt{\frac{\pi \log e}{E_m}} \tag{C.21}$$

$$B = \frac{CR_t/E_m}{C - R_t} \tag{C.13}$$

and

$$E_m = \left(\frac{1}{2} - p_o\right) \log \frac{q_o}{p_o} - C \tag{B.5}$$

2. Upper Bound to $\overline{N}$

Instead of a single probability criterion K, we can establish a set of increasingly positive criteria K_1, K_2, K_3, K_4, ... , where

$$K_j = K_1 + (j - 1)\,\Delta K \tag{C.22}$$

Let us next consider a decoding computer which searches through the truncated message set S_f according to the following rules, adopted in Chapter IV.

(a) The computer begins with the smallest criterion K_1, and starts out to generate sequentially the entire set S_f. As the computer proceeds, it discards any sequence which differs from the received message in more than k_n digits out of n.

(b) As soon as the computer discovers any sequence in S_f which

is retained through length $n = n_f$, it prints the corresponding first information digit.

(c) If the complete set S_f is discarded, the computer adopts the next larger criterion (K_2), and starts over again from the beginning. It continues this procedure until <u>some</u> sequence in S_f <u>is</u> retained through length $n = n_f$. It then prints the corresponding first information digit.

(d) The decoder repeats the above procedure in its entirety for each successive information digit in turn.

We are interested in establishing an upper bound to the ensemble average number $\bar{N}$ of binary computations which must be performed upon the subset S_1 of incorrect messages, when the decoding computer proceeds in accordance with the rules stipulated above.

A probability criterion K_j (for $j \geq 2$) is never used unless the entire set S_f — and therefore the correct message s_o — is discarded for criterion K_{j-1}. If the correct message s_o is to be discarded, then more than k_n transmission errors must occur, for some length $n \leq n_f$. Each probability criterion K_j and its associated distance criterion k_n are so related, through Eqs.(B.22) and (B.24), that

$$P_j(d_o > k_n) \leq 2^{-k_j} \qquad \text{(for all n)} \qquad \text{(C.23)}$$

where d_o represents the actual number of transmission errors. There are n_f different lengths at which the correct message s_o could be discarded. Since the probability of a union of events can be no larger than the sum of their individual probabilities, we have the result that

$$P_j\ (s_o \text{ discarded}) \leqslant n_f 2^{-K_j} \tag{C.24}$$

The probability that the decoding computer uses criterion K_j is therefore

$$P(j) \leqslant n_f 2^{-K_{j-1}} \qquad (j \geqslant 2) \tag{C.25}$$
$$= 1 \qquad (j = 1)$$

Let $\bar{N}_j$ denote the average number of computations required to eliminate the entire subset S_1, when the computer uses criterion K_j. In defining $\bar{N}_j$, we average over the ensemble of all possible convolutional generator sequences g. In order to find $\bar{N}$, we must next average over j — that is, over the (statistically independent) ensemble of transmission errors.

$$\bar{N} = \sum_j P(j)\, \bar{N}_j \tag{C.26}$$

Since these two averaging operations are statistically independent, they could be interchanged without affecting the result. Accordingly, $\bar{N}$ does in fact have the significance attributed to it, and represents the average number of binary computations required by the specified computer to eliminate the incorrect subset S_1, where the final averaging is over the ensemble of possible generator sequences.

Rough Bound to $\bar{N}$. Substituting Eqs.(C.14) and (C.25) in Eq. (C.26), we have

$$\bar{N} < D_1 n_f 2^{K_1 B} + D_1 n_f^2 \sum_{j=2} 2^{K_j B} \cdot 2^{-K_{j-1}} \tag{C.27}$$

This equation can be evaluated with the help of Eq.(C.22).

$$\bar{N} < D_1 n_f \left[2^{K_1 B} + n_f 2^{K_1(B-1)+\Delta K} \sum_{j=2} 2^{(j-1)\Delta K(B-1)} \right] \qquad (C.28)$$

The summation on j is bounded by the infinite sum, which converges for $B < 1$.

$$\bar{N} < D_1 n_f \left[2^{K_1 B} + n_f 2^{K_1(B-1)} \frac{2^{\Delta K B}}{1 - 2^{\Delta K(B-1)}} \right] \quad (\text{for } B<1) \qquad (C.29)$$

The definition of K_j given in Eq.(C.22) is somewhat arbitrary, but does serve to permit simple minimization of the r.h.s. of Eq. (C.29) with respect to K_1 and ΔK. These minimizing values are found to be

$$\Delta K = \frac{\log B}{B - 1} \qquad (C.30)$$

$$K_1 = \log \frac{n_f}{B^{1/1-B}} \qquad (C.31)$$

When these values are substituted into Eq.(C.29), we obtain finally the rough bound that

$$\bar{N} < n_f^{(1+B)} \cdot \frac{D_1}{1 - B} \cdot \left(\frac{1}{B}\right)^{B/1-B} \quad (\text{for } B<1) \qquad (C.32)$$

The constraint that $B < 1$ is satisfied for rates of transmission such that

$$R_t < \frac{C}{1 + \frac{C}{E_m}} \qquad (C.33)$$

where C is the channel capacity.

Tight Bound to $\bar{N}$. We can obtain a tighter bound on $\bar{N}$ by using the tight bound on $\bar{N}_j$ given by Eq.(C.18).

$$\frac{1}{D_1}\bar{N} < (D_2 + D_3)\left[2^{K_1 \frac{R_t}{E_m}} + n_f 2^{K_1\left(\frac{R_t}{E_m} - 1\right)+\Delta K} \sum_{j=2} 2^{(j-1)\Delta K\left(\frac{R_t}{E_m} - 1\right)}\right]$$

$$+ 2^{K_1 B} + n_f 2^{K_1(B-1)+\Delta K} \sum_{j=2} 2^{(j-1)\Delta K(B-1)}$$

$$+ D_4\left[\sqrt{K_1}\, 2^{K_1 B} + n_f 2^{K_1(B-1)+\Delta K} \sum_{j=2} \sqrt{K_1 + (j-1)\Delta K}\; 2^{(j-1)\Delta K(B-1)}\right]$$

The last summation can be bounded by use of the inequality

$$\sqrt{K_1 + (j-1)\Delta K} \leqslant \frac{K_1 + (j-1)\Delta K}{\sqrt{K_1 + \Delta K}}$$

We obtain finally the result that

$$\bar{N} < D_1\left[(D_2 + D_3)2^{K_1 \frac{R_t}{E_m}} + (1 + D_4\sqrt{K_1})2^{K_1 B}\right]$$

$$+ n_f D_1\left\{(D_2 + D_3)2^{-K_1\left(1 - \frac{R_t}{E_m}\right)}\left(\frac{2^{\Delta K \frac{R_t}{E_m}}}{1 - 2^{-\Delta K(1 - R_t/E_m)}}\right)\right.$$

$$\left. + 2^{-K_1(1-B)}\left(\frac{2^{\Delta K B}}{1 - 2^{-\Delta K(1-B)}}\right)\left[1 + \frac{D_4}{\sqrt{K_1 + \Delta K}}\left(K_1 + \frac{\Delta K}{1 - 2^{-\Delta K(1-B)}}\right)\right]\right\} \tag{C.34}$$

In principle, the r.h.s. of Eq.(C.34) may also be minimized with respect to K_1 and ΔK. The expression is sufficiently complicated, however, that numerical trial-and-error methods provide the easiest approach. To a good approximation, the minimizing values of K_1 and ΔK given in Eqs.(C.30) and (C.31) are still substantially optimum.

Substitution of these values into Eq.(C.34) results in an expression which reveals explicitly the dependence of $\overline{N}$ upon code length n_f. The term which varies most rapidly with n_f involves $n_f\sqrt{K_1}\ 2^{-K_1(1-B)}$. For $K_1 = \log \frac{n_f}{B^{1/1-B}}$, we have

$$\overline{N} < D_5 n_f^{\,B} \sqrt{\log D_6 n_f} \tag{C.35}$$

where D_5 and D_6 are constants independent of n_f.

3. Bound on $\Delta(n)\left|S_1(n)\right|$

The tree-structure of the convolutional message set S_f, illustrated in Fig. 4-1, is such that the number of digits $\Delta(n)\left|S_1(n)\right|$ which the decoding computer must generate in order to extend the entire subset S_1 from length n to length $(n+1)$ depends upon whether or not n corresponds to a node point. There are n_0R_t nodes in each branch of length n_0.

At length $n = \ell n_0$, where ℓ is an integer, there are exactly $2^{\ell n_0 R_t - 1}$ messages in S_1. In general, at length $n = \ell n_0 + i$,

$$\left|S_1(\ell n_0 + i)\right| = \begin{cases} 2^{\ell n_0 R_t + i - 1} & (\text{for } 0 \leqslant i < n_0 R_t) \\ 2^{(\ell+1) n_0 R_t - 1} & (\text{for } n_0 R_t \leqslant i < n_0) \end{cases} \tag{C.36}$$

Each sequence of length n generates two sequences of length $(n+1)$ whenever n corresponds to a node. Otherwise, each sequence merely extends one digit in length. Since $\Delta(n)$ is the number of new digits that must be generated per sequence for each unit extension,

$$\Delta(\ell n_0 + i) = \begin{cases} 2 & (\text{for } 0 \leqslant i < n_0 R_t) \\ 1 & (\text{for } n_0 R_t \leqslant i < n_0) \end{cases} \tag{C.37}$$

Combining Eqs.(C.36) and (C.37), we have

$$\left.\begin{aligned} \Delta(\ell n_o + i)\left|S_1(\ell n_o + i)\right| &= 2^{\ell n_o R_t + i} \qquad (\text{for } 0 \leqslant i < n_o R_t) \\ &= 2^{(\ell+1) n_o R_t - 1} \qquad (\text{for } n_o R_t \leqslant i < n_o) \end{aligned}\right\} \quad (C.38)$$

In Section 1 of this appendix we obtain the bound

$$\left|S_1(n)\right| \leqslant D_o 2^{nR_t} \quad (C.5)$$

where

$$D_o = \frac{1}{2} 2^{(n_o-1)R_t} \quad (C.6)$$

Accordingly, for $n = \ell n_o + i$, we have

$$\left|S_1(\ell n_o + i)\right| \leqslant 2^{(\ell+1) n_o R_t + (i-1)R_t - 1} \qquad (\text{for } 0 \leqslant i < n_o) \quad (C.39)$$

We postulate that the overbound given by Eq.(C.5) is sufficiently gross that

$$\Delta(n)\left|S_1(n)\right| \leqslant D_o 2^{(n+1)R_t} \quad (C.40)$$

Again writing n in the form $\ell n_o + i$, we have from Eq.(C.40),

$$\Delta(\ell n_o + i)\left|S_1(\ell n_o + i)\right| \leqslant 2^{(\ell+1) n_o R_t + iR_t - 1} \qquad (\text{for } 0 \leqslant i < n_o) \quad (C.41)$$

Since $n_o R_t$ is constrained by diophantine considerations to be a positive integer, comparison of the r.h.s. exponents of Eqs.(C.38) and (C.41) verifies the postulate of Eq.(C.40). Subtracting the term $\ell n_o R_t$ from each exponent, we are left with the true inequalities

$$i \leqslant (n_o R_t - 1) + iR_t \qquad (\text{for } 0 \leqslant i < n_o R_t) \quad (C.42)$$

and

$$n_o R_t - 1 < (n_o R_t - 1) + iR_t \qquad (\text{for } n_o R_t \leqslant i < n_o) \quad (C.43)$$

Appendix D: ESTIMATION OF COMPUTATION CUT-OFF LEVELS

1. Determination of $\lambda_j^*(n)$

In Chapter VI, we are confronted with the problem of determining a set of computation cut-off levels L_j, such that the probability that more than L_j binary computations are required to eliminate the incorrect message subset S_1 is no greater than the probability $P(e_1)$ that any incorrect message lies closer than the received message to the transmitted sequence s_o. In equation form, we seek a set of numbers L_j satisfying the inequality

$$P(N_j > L_j) \leqslant P(e_1) \tag{6.4}$$

where N_j is the number of computations actually needed to successfully discard S_1 in any particular experiment.

On account of the statistical constraints between sequences in S_1, exact determination of suitable levels L_j is difficult. As pointed out in Chapter VI, however, by means of neglecting these interdependencies it is possible to obtain a set of estimated levels L_j^*.

Let us consider a block code specifically designed to contain $\left|S_1(n)\right|$ messages, each of which is selected independently at random with replacement from the set of all binary sequences of length n. Averaging over this ensemble of all 2^n possible messages, we have from Appendix B the result that

$$P(d_i \leqslant k_n) \leqslant 2^{-nR_K(n)} \qquad (\text{for } k_n \leqslant \tfrac{1}{2} n) \tag{B.26}$$

where d_i is the distance between the i^{th} message of the code set

and any particular received sequence. This equation is identical with the corresponding result for convolutional coding, and $R_K(n)$ and k_n are related to the probability criterion K by the geometric construction of Fig. 4-2. Given that $K = K_j$, we rewrite Eq.(B.26) as

$$P_j(d_i \leqslant k_n) \leqslant 2^{-R_j(n)} \qquad (\text{for } k_n \leqslant \tfrac{1}{2} n) \tag{D.1}$$

where $R_j(n)$ means $R_K(n)$ evaluated for $K = K_j$. The ensemble average number $\overline{M}_j(n)$ of sequences that are probable according to criterion K_j is therefore the same as in the case of convolutional coding discussed in Appendix C.

$$\overline{M}_j(n) = \left|S_1(n)\right| \cdot P_j(d_i \leqslant k_n) \tag{C.7}$$

In accordance with the discussion of Chapter VI, in order to evaluate suitable L_j^* we wish first to determine a set of functions $\lambda_j^*(n)$ such that, for every positive integral value of j and n,

$$P_r\left[M_j(n) > \lambda_j^*(n)\overline{M}_j(n)\right] \leqslant P(e_1) \tag{6.13}$$

The sub-r notation is used in Chapter VI to distinguish a probability on the ensemble of random block codes, and is neither needed for clarity nor used hereafter. Equation (6.13) is actually a set of requirements, one for each allowed value of j and n.

Equation (A.30) in Appendix A states an upper bound on the probability of more than np successes in n independent experiments, each of which has probability p_o of success. For convenience, we rewrite that equation using the logarithmic base e instead of 2.

$$P(d_o > np) \leqslant e^{-n\left[H_e(p_o)-H_e(p)+(p-p_o)\log_e\frac{q_o}{p_o}\right]} \qquad (\text{for } p > p_o) \tag{D.2}$$

where d_o is the actual number of success in n tries, and $q_o = 1 - p_o$.

Now let P_j stand for $P_j(d_i \leqslant k_n)$, and $Q_j = 1 - P_j$. We can make the following identifications.

$$\begin{aligned} d_o &= M_j(n) \\ n &= \left| S_1(n) \right| \\ p &= \mu \\ p_o &= P_j \\ q_o &= Q_j \end{aligned}$$

Then Eq.(D.2) goes into

$$P\left[M_j(n) > \mu \left| S_1(n) \right|\right] \leqslant e^{-\left|S_1(n)\right|\left[H_e(P_j)-H_e(\mu)+(\mu-P_j)\log_e \frac{Q_j}{P_j}\right]} \qquad (\text{for } \mu > P_j) \qquad (D.3)$$

The exponent in Eq.(D.3) can be rewritten, letting $\nu = 1 - \mu$.

$$P\left[M_j(n) > \mu \left| S_1(n) \right|\right] \leqslant e^{-\left|S_1(n)\right|\left[\mu\log_e \frac{\mu}{P_j} + \nu \log_e \frac{\nu}{Q_j}\right]} \qquad (\text{for } \mu > P_j) \qquad (D.4)$$

Next expand $\nu \log_e \frac{\nu}{Q_j}$, in terms of μ and P_j , by a Taylor's series.

$$\log_e \frac{\nu}{Q_j} = -(\mu - P_j)\left[1 + \frac{1}{2}(\mu + P_j) + \frac{1}{3}(\mu^2 + \mu P_j + P^2) + \ldots\right] \qquad (D.5)$$

Since $\mu > P_j > 0$, $\frac{1}{2}(\mu + P_j) < \mu$, and similarly each term in brackets above is less than in the geometric series expansion of $\frac{1}{1-\mu}$. Therefore,

$$\nu \log_e \frac{\nu}{Q_j} = (1-\mu)\log_e \frac{\nu}{Q_j} > -(\mu - P_j) \qquad (D.6)$$

Substituting Eq.(D.6) into Eq.(D.4), we strengthen the inequality.

$$P\left[M_j(n) > \mu \left| S_1(n) \right|\right] < e^{-\left|S_1(n)\right|\left[\mu \log_e \frac{\mu}{P_j} - (\mu - P_j)\right]} \quad (\text{for } \mu > P_j) \tag{D.7}$$

Finally, let us define

$$\lambda_j^* = \frac{\mu}{P_j} \tag{D.8}$$

Then, using Eq.(C.7), we have

$$\mu \left| S_1(n) \right| = \lambda_j^* \bar{M}_j(n) \tag{D.9}$$

and accordingly,

$$P\left[M_j(n) > \lambda_j^* \bar{M}_j(n)\right] < e^{-\bar{M}_j(n)\left[\lambda_j^* \log_e \lambda_j^* + 1 - \lambda_j^*\right]} \quad (\text{for } \lambda_j^* > 1) \tag{D.10}$$

The ℓ.h.s. of Eq.(D.10) is equivalent to that of Eq.(6.13). For a given value of j and n, we can equate the right-hand sides of these two equations, and solve for λ_j^*. The sets of values of λ_j^* determined in this fashion then define functions $\lambda_j^*(n)$ such that the conditions imposed by Eq.(6.13) are satisfied.

For simplicity of notation, define

$$f(\lambda_j^*) = \lambda_j^* \log_e \lambda_j^* + 1 - \lambda_j^* \tag{D.11}$$

and

$$P(e_1) = e^{-\alpha} \tag{D.12}$$

The requirement on λ_j^* then becomes

$$\bar{M}_j(n)\, f(\lambda_j^*) = \alpha \tag{D.13}$$

A plot of the function $f(\lambda_j^*)$ is given in Fig. D-1.

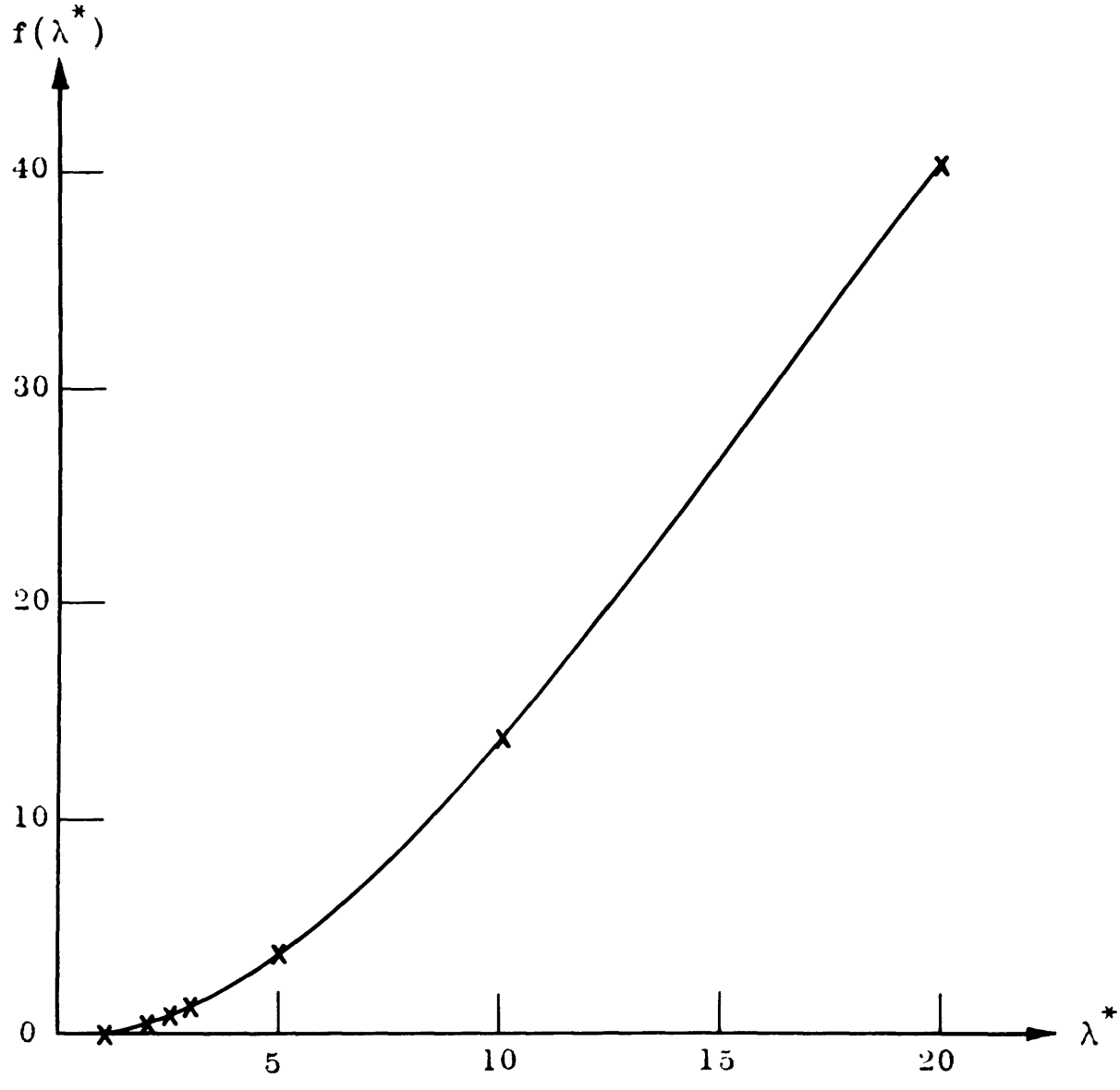

Figure D-1

PLOT OF $f(\lambda^*)$

2. Evaluation of L_j^*

We are seeking to evaluate the set of estimated computation cut-off levels L_j^*, defined in Chapter VI as

$$L_j^* = \sum_{n=1}^{n_f} \Delta(n)\, \lambda_j^*(n)\, \bar{M}_j(n) \qquad (6.16)$$

where, as in Appendix C, $\Delta(n)$ is the number of additional binary digits in the case of convolutional coding which the decoding computer must generate per probable sequence of length n, in order to progress to length $(n+1)$. The values $\lambda_j^*(n)$ are to be determined in accordance with the transcendental equation (D.13).

General Behavior. Actual evaluation of L_j^* requires numerical methods. It is possible, however, to gain considerable insight into the nature of L_j^* by observing the general characteristics of the summand in Eq.(6.16). The factor $\bar{M}_j(n)$, illustrated in Fig. 4-4, has a single maximum term, which is shown in Appendix C to be bounded by

$$M_j(n) < D_o 2^{K_j B} \qquad (D.14)$$

where

$$D_o = \frac{1}{2} 2^{(n_o-1)R_t} \qquad (C.11)$$

Now consider the function $\lambda_j^*(n)\bar{M}_j(n)$, and differentiate with respect to $\bar{M}_j(n)$. Using simplified notation, we have

$$\frac{d}{d\bar{M}} (\lambda^* \bar{M}) = \lambda^* + \bar{M} \frac{d\lambda^*}{d\bar{M}} \qquad (D.15)$$

We may also differentiate Eq.(D.13) with respect to $\bar{M}_j(n)$, where

it is understood that only n and j are to be considered variable. This is important, since although $P(e_1)$ and therefore α are constants with respect to n and j, they are variables with respect to n_f, p_o, and R_t. With this restriction,

$$f(\lambda^*) + \bar{M}\, f'(\lambda^*)\, \frac{d\lambda^*}{d\bar{M}} = 0 \qquad (D.16)$$

where the prime denotes differentiation with respect to the argument. From Eqs.(D.16) and (D.15) we obtain the results

$$d(\lambda^* \bar{M}) = \frac{\lambda^* - 1}{\log_e \lambda^*}\, d\bar{M} \qquad (\text{for } \lambda^* > 1) \qquad (D.17)$$

and

$$d\lambda^* = -\frac{f(\lambda^*)}{\log_e \lambda^*} \cdot \frac{d\bar{M}}{\bar{M}} \qquad (D.18)$$

From these two equations it is apparent that, for fixed n_f, p_o, and R_t, the function $\lambda_j^*(n)\, \bar{M}_j(n)$ must have the same general shape as $\bar{M}_j(n)$, with a single maximum term which occurs for given j at the same value of n. We note also that $\lambda_j^*(n)\, \bar{M}_j(n)$ is a monotonically increasing function of $\bar{M}_j(n)$, but that the required multiplying factor $\lambda_j^*(n)$ itself decreases as $\bar{M}_j(n)$ increases. These relations are all in natural agreement with intuition.

A sketch of an upper bound on $\lambda_j^*(n)\, \bar{M}_j(n)$, derived from the bound on $\bar{M}_j(n)$, is given in Fig. D-2. For small values of n, it is the curve $\left|S_1(n)\right| \approx D_o 2^{nR_t}$ which is significant, since Eq.(6.13) is automatically satisfied when every sequence in the message set is retained.

A bound on the ensemble average number of binary computations

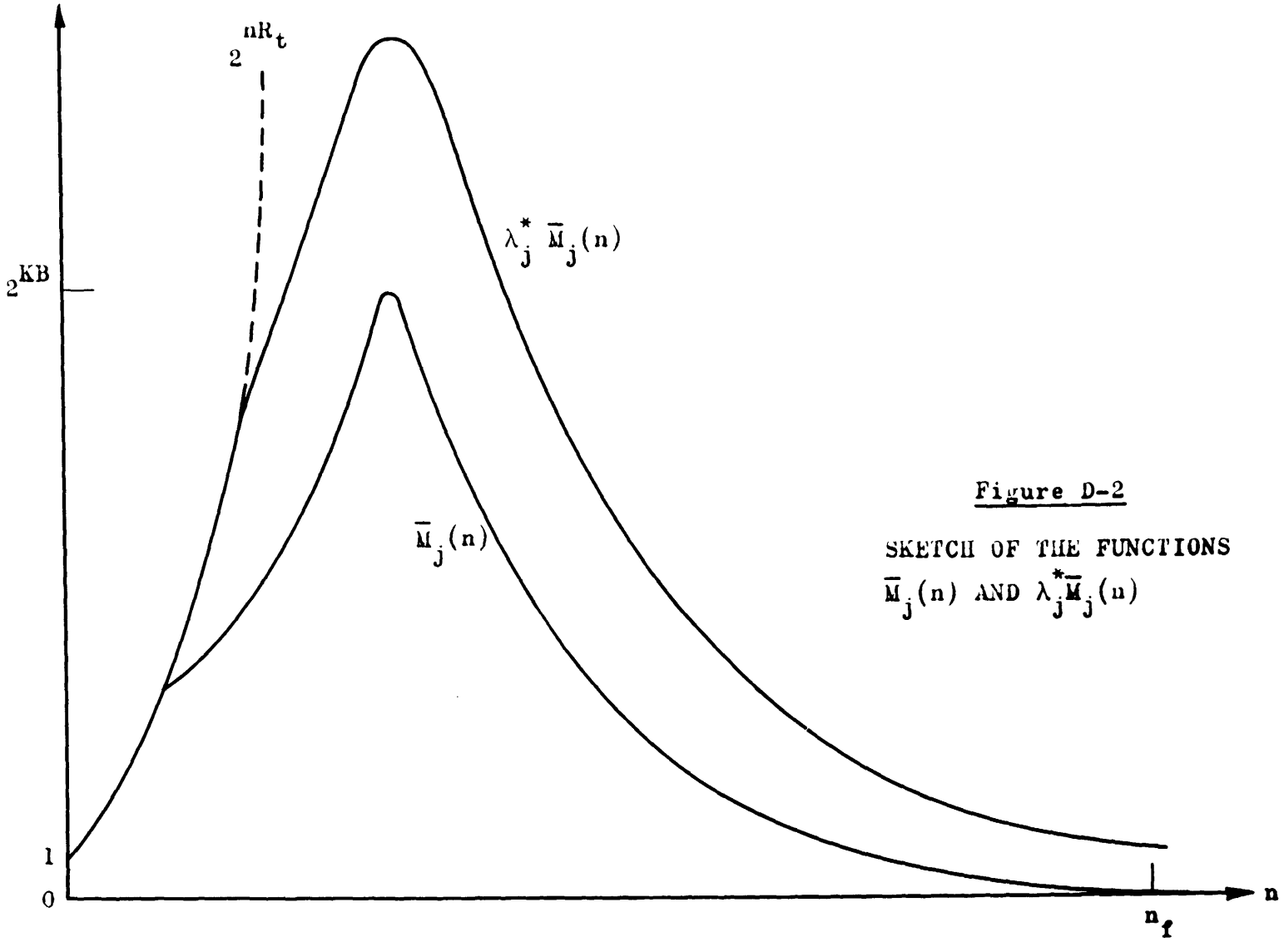

Figure D-2

SKETCH OF THE FUNCTIONS $\bar{M}_j(n)$ AND $\lambda_j^* \bar{M}_j(n)$

required to eliminate the incorrect subset S_1 is derived in Appendix C.

$$\bar{N}_j \leqslant \sum_{n=1}^{n_f} \Delta(n)\, \bar{M}_j(n) \qquad (C.9)$$

Comparison of Eqs.(C.9) and (6.16) reveals that each term in the summation for L_j^* is obtained by multiplying the corresponding term for the bound on $\bar{N}_j$ by the appropriate value $\lambda_j^*(n)$. Since the set of probability criteria K_j are chosen to form a monotonically increasing set, it follows that for fixed n

$$\bar{M}_{j+1}(n) > \bar{M}_j(n) \qquad (D.19)$$

Then, from Eq.(D.18),

$$\lambda_{j+1}^*(n) < \lambda_j^*(n) \qquad (D.20)$$

Finally, since Eq.(D.20) is true for every value of n, the ratios of L_j^* to $(\bar{N}_j)_{bound}$ must be such that

$$L_{j+1}^*/(\bar{N}_{j+1})_{bound} < L_j^*/(\bar{N}_j)_{bound} \qquad (D.21)$$

For the specific case $R_t = \frac{1}{3}$, $P(e_1) = 10^{-12}$, and $p_o = .050$, values of L_j^*, $(\bar{N}_j)_{bound}$, and $L_j^*/(\bar{N}_j)_{bound}$ obtained by numerical computation are given in Table D-1 for j = 1 to 5. In addition, a plot of $L_j^*/(\bar{N}_j)_{bound}$ is included in Chapter VI as Fig. 6-1.

TABLE D.1

j	L_j^*	$(\bar{N}_j)_{bound}$	$L_j^*/(\bar{N}_j)_{bound}$
1	4,500	1,330	3.4
2	6,600	2,350	2.8
3	10,300	4,500	2.3
4	18,000	9,300	1.9
5	30,000	19,000	1.6

Upper Bound. A bound on the behavior of L_j^* with respect to the total code length n_f can be obtained by expanding $f(\lambda_j^*)$ in a Taylor series.

$$f(\lambda_j^*) = \lambda_j^* \left[\frac{\lambda_j^* - 1}{\lambda_j^*} + \frac{1}{2} \left(\frac{\lambda_j^* - 1}{\lambda_j^*} \right)^2 + \frac{1}{3} \left(\frac{\lambda_j^* - 1}{\lambda_j^*} \right)^3 + \ldots \right] + 1 - \lambda_j^* \tag{D.22}$$

This expansion is valid for any $\lambda_j^* > \frac{1}{2}$. In our case, λ_j^* is restricted to be greater than unity, and therefore each of the bracketed terms is positive. Accordingly,

$$f(\lambda_j^*) > \frac{1}{2} \lambda_j^* - 1 \tag{D.23}$$

Substituting Eq.(D.23) into Eq.(D.13) provides an upper bound to $\lambda_j^*(n)\bar{M}_j(n)$.

$$\lambda_j^*(n)\bar{M}_j(n) < 2\,\bar{M}_j(n) + 2\alpha \tag{D.24}$$

This result can be used in Eq.(6.16), in order to bound L_j^*.

$$L_j^* < \sum_{n=1}^{n_f} 2\Delta(n)\bar{M}_j(n) + \sum_{n=1}^{n_f} 2\Delta(n)\alpha \tag{D.25}$$

From Eq. (C.9), the first summation is equal to twice $(\bar{N}_j)_{bound}$.

Since α is not a function of n, and

$$\sum_{n=1}^{n_f} \Delta(n) = n_f(1+R_t) \tag{D.26}$$

we have finally

$$L_j^* < 2(\bar{N}_j)_{bound} + 2n_f(1+R_t)\alpha \tag{D.27}$$

In Eq.(D.12), α is defined as the negative logarithm of $P(e_1)$. From Chapter V, we have

$$P(e_1) < n_f A_S P(e)_{random} \tag{5.38}$$

where $P(e)_{random}$ is the ensemble average probability of error for random block codes of length n_f, and is bounded in Appendix A. Using Eqs.(A.54) and (A.55), we can bound α by

$$\alpha < n_f E + D \tag{D.28}$$

where E is equal to E_t or E_{crit} (depending on whether or not R_t is greater than R_{crit}), and D is some (small) constant which is chosen to bound the logarithm of the coefficients in $P(e_1)$. Finally, then,

$$L_j^* < 2(\bar{N}_j)_{bound} + 2(1+R_t)n_f(n_f E + D) \tag{D.29}$$

Thus we find that the estimated computation cut-off levels L_j^* are bounded by twice the bound on the average number of computations required to eliminate the incorrect subset S_1, plus a term which grows no faster than the square of the code length.

There is a difference of almost a single power of n_f in the gross and tight bounds on $\bar{N}_j$ derived in Eqs.(C.14) and (C.18) of

Appendix C. The n_f^2 term in Eq.(D.29) corresponds to a gross bound. Unfortunately, the transcendental nature of Eq.(D.13) precludes algebraic solution, and a tighter bound on L_j^* than that given in Eq.(D.29) appears difficult to obtain. In spite of this fact, the character of the function $\lambda_j^*(n)\bar{M}_j(n)$ sketched in Fig. D-2 indicates that a considerably tighter bound exists.

The Average Cut-Off Level $\bar{L}^*$. It is also possible to bound the average value $\bar{L}^*$ of the computation cut-off levels L_j^*, by means of weighting according to the probability that a criterion K_j is used in the decoding process. We proceed as in Appendix C, where we compute a bound on the average value $\bar{N}$ of the number of binary computations required to eliminate the incorrect subset S_1.

Define

$$\bar{L}^* = \sum_j P(j)L_j^* \qquad (D.30)$$

The appropriate bound on $P(j)$ is now somewhat less than that given in Eq.(C.25), since the existence of the cut-off levels themselves introduces a way in which the decoding procedure can terminate even when the correct message sequence s_o is not discarded. If we set

$$\left.\begin{aligned} P(j) &\leqslant n_f 2^{-K_{j-1}} && (j \geqslant 2) \\ &= 1 && (j = 1) \end{aligned}\right\} \qquad (C.25)$$

however, we obtain a conservative answer.

Substituting Eqs.(C.25), (C.22), and (D.29) into Eq.(D.30), we obtain

$$\bar{L}^* < 2(\bar{N}_1)_{\text{bound}} + 2n_f \sum_{j=2} (\bar{N}_j)_{\text{bound}} \, 2^{-K_{j-1}}$$

$$+ 2(1+R_t)n_f(n_f E + D)\left[1 + n_f \sum_{j=2} 2^{-K_{j-1}}\right] \qquad (D.31)$$

The first two terms are just twice $(\bar{N})_{\text{bound}}$. The value of the summation in brackets is bounded by the infinite sum.

$$\sum_{j=2} 2^{-K_{j-1}} \leqslant \frac{2^{-K_1}}{1 - 2^{-\Delta K}} \qquad (D.32)$$

The values of K_1 and ΔK which minimize the bound on $\bar{N}$ are given in Eqs.(C.30) and (C.31). Substituting these values into Eq.(D.32), we have

$$\sum_{j=2} 2^{-K_{j-1}} \leqslant \frac{1}{n_f} \cdot \frac{B^{1/1-B}}{1 - B^{1/1-B}} \qquad (D.33)$$

Finally, therefore,

$$\bar{L}^* < 2(\bar{N})_{\text{bound}} + 2(1+R_t)n_f(n_f E + D) \frac{1}{1 - B^{1/1-B}} \qquad (D.34)$$

where

$$B = \frac{CR_t/E_m}{C - R_t} \qquad (C.13)$$

Again we find that $\bar{L}^*$ grows no more rapidly than the square of the code length n_f.

BIBLIOGRAPHY

1. Shannon, C. E., The Mathematical Theory of Communication (University of Illinois Press, Urbana, Illinois) 1949.

2. Shannon, C. E., "The Rate of Approach to Ideal Coding," Abstract only, I.R.E. Convention Record, Part IV, 1955.

3. Shannon, C. E., Unpublished seminar notes, Dept. of Elec. Engineering, Mass. Inst. of Tech., Spring, 1956.

4. Elias, P., "Coding for Noisy Channels," I.R.E. Convention Record, Part IV, 1955.

5. Elias, P., "Coding for Two Noisy Channels," Reprint from Information Theory (C. Cherry, Editor), Third London Symposium, September, 1955. (Buttersworth Scientific Publications, London, England)

6. Hamming, R. W., "Error Detecting and Error Correcting Codes," Bell System Tech. Jour., April, 1950.

7. Feller, W., Probability Theory and its Applications (John Wiley and Sons, New York, N.Y.), Chapters I and II.

8. Feinstein, A., "Error Bounds in Noisy Channels Without Memory," Trans. I.R.E., Vol. IT-1, September, 1955.

9. Reed, I. S., "A Class of Multiple-Error-Correcting Codes and the Decoding Scheme," Trans. I.R.E., PGIT-4, September, 1954.

10. Slepian, D., "A Class of Binary Signaling Alphabets," Bell System Tech. Jour., January, 1956.

11. Birkhoff and MacLane, A Survey of Modern Algebra (The Macmillan Company, New York, N.Y.) Revised Edition, 1953, Chap. VI.

12. Elias, P., "Error-Free Coding," Trans. I.R.E., PGIT-4, Sept. 1954.

13. Chernov, H., "A Measure of Asymptotic Efficiency for Tests of a Hypothesis Based on a Sum of Observations," Ann. Math. Stat., 23, 1952.

14. Cramer, H., "Sur un Nouveau Théorème-Limite de la Théorie des Probabilités," Colloque d'Octobre, 1937, sur la Théorie des Probabilités, Hermann et Cie, Paris, France, 1938.

15. Slepian, D., "A Note on Two Binary Signaling Alphabets," Trans. I.R.E., PGIT, June, 1956.