BLOCK CODING WITH NOISELESS FEEDBACK

by

Elwyn Ralph Berlekamp

B. S. Massachusetts Institute of Technology
(1962)

M. S. Massachusetts Institute of Technology
(1962)

SUBMITTED IN PARTIAL FULFILLMENT OF THE
REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

September 1964

Signature of Author _____
Department of Electrical Engineering, August 24, 1964

Certified by _____
Thesis Supervisor

Accepted by _____
Chairman, Departmental Committee on Graduate Students

BLOCK CODING WITH NOISELESS FEEDBACK

by

ELWYN RALPH BERLEKAMP

Submitted to the Department of Electrical Engineering
on August 24, 1964, in partial fulfillment of the
requirements for the degree of Doctor of Philosophy

ABSTRACT

This thesis is concerned with the use of block codes to transmit information over two-way communication systems which have a discrete, memoryless, noisy channel in the forward direction and a reverse channel which is noiseless and undelayed and has unlimited capacity. It has been known that the capacity in the forward direction is not increased by the reverse channel. It has also been known that the probability of error approaches zero exponentially with increasing block length at any fixed rate less than capacity. For a region of rates between a critical rate and capacity, it has been known that the exponent with which the probability of error approaches zero cannot be improved by the use of feedback, and there was some question whether the feedback channel could be made to serve any useful purpose at all, either to improve the probability of error or to decrease the complexity of the coding and decoding operations.

In view of these results, we focus our primary attention on low rate codes, including zero-rate codes whose block length approaches infinity while the number of codewords remains fixed. We succeed in obtaining several new and improved bounds on the probability of error for such codes, both with and without feedback.

We evaluate the zero-rate exponents for arbitrary one-way channels. This new general result leads to improved lower bounds on the probability of error at low rates, via techniques recently introduced by C. E. Shannon and R. G. Gallager. We evaluate the zero-rate exponent for large classes of feedback channels, including all binary-input channels which satisfy certain symmetry requirements. These results lead to strengthened bounds on the probability of error for channels with feedback. We find that at low rates it is possible to obtain substantially improved error probabilities with the use of feedback. Although our results may be invalidated if the feedback channel is noisy, we show that the results are not effected by a delay in the feedback channel unless the delay is comparable to the block length.

Several constructive feedback coding strategies are presented. Using elaborate inductive arguments, we derive a class of coding strategies which are asymptotically optimum for the binary symmetric channel with feedback over a large region of rates. It is felt that these strategies could be profitably applied to problems in the statistical design of experiments whenever the situation is such that successive experiments may be modified according to the results of previous ones. Most previous studies in the statistical design of experiments have not permitted such modifications. By utilizing this "feedback", we not only find that it is possible to achieve much smaller error probability, but we show how.

Thesis Supervisor: Robert G. Gallager
Title: Associate Professor of Electrical Engineering

Preface

This thesis is directed toward the problem of block coding with noiseless feedback, at low rates. For comparison, a chapter (2) on block coding without feedback is included, containing several new results. In chapter 3 we attack the zero-rate coding problem for channels with noiseless feedback, and in Chapter 4 we consider the construction of coding strategies for the binary symmetric channel with noiseless feedback.

Familiarity with the material summarized in the introductory Chapter 1 is the sole prerequisite to any of the other chapters. The three final chapters are sufficiently independent of each other that any of these chapters may be read with a minimum of reference to the others. Although the results of these chapters are related, it is expected that they will appeal to different groups. Chapter 2 will be of primary interest to the error exponent theorists of the Shannon-Fano tradition; Chapter 4 will be of greater interest to algebraists and number theorists interested in problems relating to the statistical design of experiments. Chapter 3 may have an intermediate appeal.

Despite restraining efforts by the author, a large number of symbols are introduced. To aid the forgetful reader, an included glossary tabulates each of these symbols, together with its definition and/or the page where the definition may be found.

To curtail errors which tend to be introduced by continual revision of the manuscript, the formulas have been numbered by the decimal system. (2.055 occurs between 2.05 and 2.06.)

Research on most of the problems discussed in this thesis is still underway. The author expects to write various papers including these (and, hopefully, stronger) results in the next year. For this reason, the author would greatly appreciate any and all comments and suggestions, helpful, critical, or otherwise.

Acknowledgement

I am glad to have this opportunity to acknowledge the thoughtful help and guidance which I have received from my graduate area committee and my thesis committee: Profs. Gallager, Shannon, Wozencraft, and Elias.

Prof. Peter Elias first triggered my interest in information theory when he was my sophomore registration officer. This past year he has found time to follow portions of this research closely enough to make several helpful suggestions, in spite of his busy schedule as head of the electrical engineering department.

Prof. John M. Wozencraft has served as my registration officer throughout graduate school. His thoughtful comments have resulted in considerable improvement in certain parts of this thesis, particularly Chapter 1.

Prof. Claude E. Shannon originated the problem toward which this thesis is directed. He also supplied several of the included examples. His inexhaustible store of novel ideas has proved most inspiring to me, as well as to everyone else in this field.

Prof. Robert G. Gallager, my thesis advisor, has closely followed all of this research. His ready availability, continued guidance, and knack for quickly dispelling erroneous ideas have kept me out of many a blind alley. His proofreading of this thesis and his detailed checking of many of the calculations have proved invaluable. Had it not been for Prof. Gallager's continued assistance, this thesis would contain many more bugs and far fewer results.

I am also indebted to various other persons at MIT and Bell Telephone Laboratories, too numerous to be mentioned, for helpful discussions on many points.

TABLE OF CONTENTS

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF CONTENTS
(continued)

TABLE OF FIGURES

(Continued on next page)

TABLE OF FIGURES

(Continued from previous page)

GLOSSARY OF SYMBOLS AND TERMS

Page Defined	Symbol	Definition	Region of Applicability
	A	a constant	
129	$A_{i,j}$	entry in Figure 4-8	
129	$\underline{A}_{i,j}$	state consisting of entires in a column of Figure 4-8	
1	a_k	channel input symbol	
1	b_j	channel output symbol	
123	borderline		
1	C	channel capacity	
3	C_o	zero-error capacity	
5	C_o^+	Rate at which $E_{sp}(R)$ becomes infinite	
	channel	See Shannon (1948)	
48	Coder	partnership including transmitter and receiver	
57	crossover	Nature's strategy change	
52	crossunder		
66	crossunder, details		
75	crossunders; single, multiple, or degenerate		
26	$D(\underline{x}_m, \underline{x}_{m'})$	distance between words $\underline{x}_m$ and $\underline{x}_{m'}$	
26	D_{min}	minimum distance	
25	$d_{i,k}$	distance between input symbols	
26	d_{max}	maximum distance between input symbols	
104	distance, Hamming		Ch 4
17	distance, for pairwise reversible channels		Ch 2
25	distance, general		Ch 2
29	dominance		
123	doublet		
3	$E(0)$	error exponent at infinitesmal rate	
2	$E(R)$	error exponent at rate R	
14	$E(\underline{x},\underline{x}')$	error exponent between codewords $\underline{x}$ and $\underline{x}'$	
6	$E_{exp}(R)$	expurgated bound on E(R)	
2	E_M	error exponent for M codewords	
3	$E_{rand}(R)$	random coding bound on E(R)	
3	$E_{sp}(R)$	sphere packing bound on E(R)	
5	$E_o(\rho)$	function introduced by Gallager	
3	E_∞	error exponent for many codewords	

GLOSSARY OF SYMBOLS AND TERMS
(continued)

Page Defined	Symbol	Definition	Region of Applicability
	e	=2.718281828...	p 73
	e	number of errors made by BSC	all other
56	e_{ig}	ignorable number of errors	
104	error correction capability		
2 104	error exponent		
	exp(x)	$=e^x$; e=2.718281828...	
2	F(0)	feedback exponent at infinitesmal rate	
2	F(R)	feedback exponent at rate R	
2	F_M	feedback exponent for M codewords	
2	F_∞	feedback exponent for many codewords	
129	f	correctable error fraction; f=e/N	
129	f_o		
129	f_t		
129	g	=1-f	
129	g_o	$=1-f_o$	
129	g_t	$=1-f_t$	
	H(x)	=-x ln x -(1-x) ln (1-x)	Ch 1, Ch 2
	H(x)	=-x log x - (1-x) log (1-x)	Ch 3, Ch 4
69	H_i	number of heavy falls in ith region	
37 47	Hamming-metric channels		
	I	Roman numeral	iff subscript
	I	integer	all other
	i	an integer	
	iff	if and only if	
1	J	number of channel outputs	
	j	an integer	
1	K	number of channel inputs	Ch 1, Ch 2
	K	an integer	Ch 3, Ch 4
	k	an integer	Ch 1, Ch 2
	k	an integer, or number of falls of a particular type	Ch 3
	k	an integer, or (log M)= RN	Ch 4
55	k_{max}		
44	L	size of a decoding list	
69	L_i	number of light falls in ith region	

GLOSSARY OF SYMBOLS AND TERMS
(continued)

Page Defined	Symbol	Definition	Region of Applicability
	l.u.b.	least upper bound	
	log	$\log_2$	
123	losing state		
	ln	$\log_e$; e = 2.718281828...	
1	M	number of codewords	
18	$\underline{M}(n)$	vector specifying composition of nth column	
44	m_n		
44	$\bar{m}_n$	upper bound on m_n	
	max	the maximum of	
	min	the minimum of	
1	N	block length	
44	N_1	a certain fraction of the block length	
59	N_a	number of questions after final crossunder	
59	N_b	number of questions before final crossunder	
11	$N_{i,k}$		
17	$N_{i,k}^{(m,m')}$		
48	Nature	Controller of channel transitions	
52	order strategies		
5	$\underline{P}$	probability vector	
15	$\underline{P}^*$	the optimum probability vector	
1	P_e	probability of decoding error	
	p	$= p_{1,2} = p_{2,1}$	Ch 4
	p	a probability	all other
1	$p_{j,k}$	channel transition probability	
28	$\underline{p}(n)$	composition of nth column before halving	
28	$\underline{p}'(n)$	composition of nth column after halving	
28	$\bar{\underline{p}}$	average of $\underline{p}(n)$	
16	pairwise reversible		
23	pairwise uniform		
48 121	partition		
110	probability strategy		

GLOSSARY OF SYMBOLS AND TERMS
(continued)

Page Defined	Symbol	Definition	Region of Applicability
11	$Pr(\underline{x}\ \underline{x}')$	probability of confusing $\underline{x}$ and $\underline{x}'$	
	q	$= p_{1,1} = p_{2,2}$ for BSC	Ch 4
	q	a probability	all other
1	R	information rate in nats	Ch 1,2,&3
	R	information rate in bits	Ch 4
4	R_{comp}		
4	R_{crit}		
	R_i	the ith region	
4	R_o		
28	$\underline{r}(n)$	$= \underline{p}'(n) - \underline{p}(n)$	
68 77	region		
81	region; deep, shallow		
71 87	s	slack	pp 71-91
	s	a variable	all other
71 81	s'	slack	
123	singlet		
71 81	slack		
120	state		
120	substate		
90	symmetric	binary-input channel	
64	T	delay	
127	$T(\underline{x})$	translation of state $\underline{x}$	
[illegible]	trajectory	See Figures 3-4	pp 50-53
127	translation bound		
	TUC	ternay unilateral channel, Fig. 2-6	
11	$u_{i,k}(s)$		
20	u_{min}		

GLOSSARY OF SYMBOLS AND TERMS
(concluded)

Page Defined	Symbol	Definition	Region of Applicability
126	$V_n(\underline{c})$	volume of n-state $\underline{c}$	
126	volume		
47	W_1	top word	
47	W_I	word which was on top at some given point	
123	winning		
	x	a variable	
	$\underline{x}$	transmitted sequence	Ch 1, Ch 2
	$\underline{x}$	a state	Ch 4
50	x_1	number of votes against top word	Ch 3,
53	$x_{j,k}$	average of x_j, $x_{j+1},\cdots,x_k$	
	$\underline{y}$	received sequence	Ch 1, Ch 2
	$\underline{y}$	state	Ch 4
70	Δ_i	difference across ith region	
29	ΔV	change in variance at a halving	
	ϵ	a negligible, not necessarily infinitesmal number	
20	λ	LaGrange multiplier	
	π	product	
	ρ	dummy variable	
	Σ	sum	
	$\star$	event	Appendix
	$\star$	the optimum	all other
	$\cup$	union of events	
	Ω	intersection of events	
	$\dagger$	footnote	
	†	footnote	

Chapter 1

HISTORICAL BACKGROUND

This thesis is concerned with the transmission of information over discrete memoryless channels having K inputs $(a_1, \ldots, a_K)$, J outputs $(b_1, \ldots, b_J)$, and a known probability transition matrix, $p_{j,k} = \Pr(b_j/a_k)$. The source selects one of $M = \exp RN$ equiprobable messages. The coder at the source then attempts to inform the decoder at the receiver which message was chosen by sending a sequence of N symbols across the noisy channel. N is the block length; R is the information rate in nats.

We consider this problem in two different cases. In the feedback case, the communication system also includes a reverse channel, running from the receiver back to the source, which is noiseless and delayless and has an unlimited capacity. The receiver uses this channel to keep the source informed of the received symbols; the transmitter is then permitted to utilize this feedback information (as well as the selected message) in deciding which symbol to transmit next. In the conventional one-way case, there is no reverse channel at all, and the transmitter must select all N transmitted symbols independently of what the source receives. In either case, after the entire block of N symbols is received, the decoder selects that message which appears most probable. If this choice does not coincide with the message selected by the source, the decoder has committed a decoding error. We are interested in the behavior of P_e, the probability of decoding error, for various channels when the source and the receiver use the best possible coding strategy.

The behavior of P_e for large M and N and fixed R is of considerable interest. In 1948 C. E. Shannon showed that any such channel has a capacity, C, with the property that for any fixed $R < C$, P_e goes to 0 with increasing M and N, but for any

fixed $R > C$, P_e remains bounded away from zero for all M and N. Later Wolfowitz (1961) showed that in fact P_e goes to 1 as M and N increase with fixed $R > C$. C is the same for both the feedback and the one-way case. In 1955 A. Feinstein showed that for any $R < C$, the one-way P_e actually goes to 0 at least exponentially in N. Later R. M. Fano (1961) showed that in fact P_e goes to 0 exponentially. This leads to the definition

$$E(R) = \lim_{N \to \infty} \sup -1/N \ln P_e \dagger \qquad (1.01)$$

as the optimum one-way exponent, which is a function of the rate R and the channel. E(R) expresses the inherent limitations on communication at rate R, $0 < R < C$. For this reason, E(R) is of fundamental importance.

In a similar manner, we define F(R) as the optimum exponent for the same channel with feedback.

$$F(R) = \lim_{N \to \infty} \sup -1/N \ln P_e \qquad (1.02)$$

Since the source and receiver can ignore the feedback channel if they so desire, it is clear that

$$E(R) \leq F(R) \qquad \text{for all } 0 < R < C. \qquad (1.03)$$

At zero rate, these exponents are no longer well-defined, for they may depend on the manner in which M and N go to infinity. This leads to the consideration of exponents for finite numbers of words.

$E_M = \lim_{N \to \infty} -1/N \ln P_e$ for the best one-way code with M codewords ($M \geq 2$) and block length N. Likewise F_M is the corresponding quantity for the channel with feedback. Obviously $E_M \leq F_M$. Finally, we define

† This definition avoids the logical difficulty arising from the conceptual possibility that $\lim_{n \to \infty} -1/N \ln P_e$ might not exist.

$$E_\infty = \lim_{M \to \infty} E_M ; \quad E(0) = \lim_{R \to 0} E(R) \text{ and similarly} \tag{1.04}$$

$$F_\infty = \lim_{M \to \infty} F_M ; \quad F(0) = \lim_{R \to 0} F(R) \tag{1.05}$$

It is apparent that

$$E(R_2) \leq E(R_1) \leq E(0) \leq E_\infty \leq E_{m_2} \leq E_{m_1} \leq E_2$$

and

$$F(R_2) \leq F(R_1) \leq F(0) \leq F_\infty \leq F_{m_2} \leq F_{m_1} \leq F_2$$

for any

$$0 < R_1 < R_2 < C; \; 2 < m_1 < m_2 \tag{1.06}$$

For some channels, E_2 may be infinite. E(R) may be infinite for some region $0 < R < C_o \leq C$, where C_o is the zero-error capacity introduced by Shannon (1956). A channel has a positive C_o iff it has some pair of inputs which have no outputs in common. If $C_o > 0$, then $C_o \geq$ i bit.

This thesis will primarily be concerned with channels which have no zero error capacity. We shall find that if $C_o = 0$, then $F_2 < \infty$, whence E_M and F_M are finite for all M.

The function E(R) has been studied by Shannon (1959), Fano (1961), Gallager (1964) and others. Their basic results for discrete memoryless channels without zero error capacity are summarized as follows: For any R,

$$E_{rand}(R) \leq E_{exp}(R) \leq E(R) \leq F(R) \leq E_{sp}(R)$$

$E_{sp}(R)$ is the sphere packing bound.

$E_{rand}(R)$ is the random coding bound.

$E_{exp}(R)$ is the improved lower bound resulting from certain

expurgation procedures applied to random ensembles of codes.

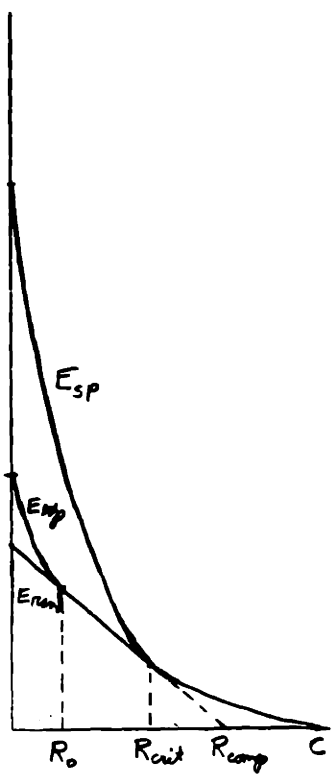
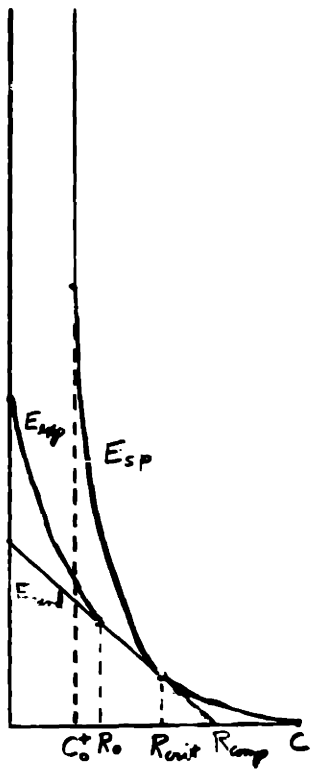
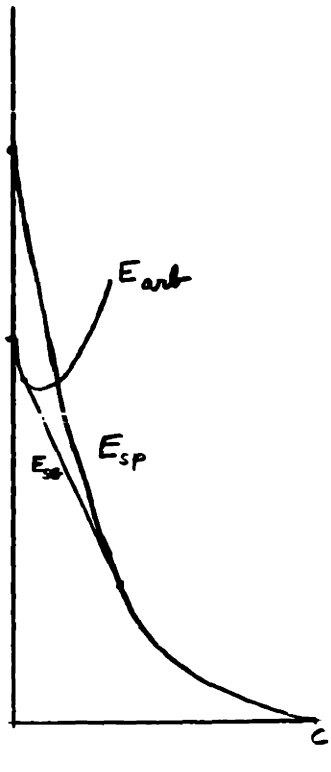


Figure 1-1



Known Bounds

Figure 1-2



New Shannon-Gallager Bound

Figure 1-3

Above some critical rate R_{crit},

$$E_{rand}(R) = E_{sp}(R) \text{ for } R_{crit} \leq R \leq C$$

Thus E(R) is known for $R_{crit} \leq R \leq C$. E(R) approaches zero parabolically as R approaches C. For sufficiently small rates, $E_{rand}(R)$ is a straight line of slope -1. $E_{rand}(0) = R_{comp}$, a rate which has significance in the sequential decoding procedures

of Wozencraft and Reiffen (1961) and Fano (1963). Except for certain pathological cases, the rate at which $E_{rand}(R)$ ceases to be a straight line of slope -1 is R_{crit}, at which $E_{rand}(R)$ joins $E_{sp}(R)$ tangentially. At a lower critical rate R_o, $E_{exp}(R)$ leaves $E_{rand}(R)$ tangentially (except, again, for certain pathological cases). In all cases $E_{exp}(R)$ approaches a higher limit than $E_{rand}(R)$. $E_{exp}(0) > E_{rand}(0)$.

For channels across which at least one output is accessible from every input, $E_{sp}(0)$ is finite, and $E_2 = F_2 \leq E_{sp}(0)$; for channels across which each output is inaccessible from at least one input, there exists a rate C_o^+ at which the sphere packing bound ceases. $E_{sp}(R) = \infty$ for $0 \leq R < C_o^+$. Clearly $C_o \leq C_o^+$. C_o^+ may be positive even when $C_o = 0$.

The most elegant derivation of these results is that given by Gallager (1964). He introduces the function $E_o(\rho)$, defined by

$$E_o(\rho) = \max_{\underline{P}} - \ln \sum_j \left(\sum_k P_k p_{j,k}^{\frac{1}{1+\rho}} \right)^{1+\rho} \tag{1.10}$$

In terms of this function, the significant rates are given by

$$C = E_o'(0) \tag{1.11}$$

$$R_{comp} = E_o(1) \tag{1.12}$$

$$R_{crit} = E_o'(1) \tag{1.13}$$

$$C_o^+ = \lim_{\rho \to \infty} E_o(\rho)/\rho = \max_{\underline{P}} - \ln \max_j \sum_{\substack{k \text{ for which} \\ p_{j,k} > 0}} P_k \tag{1.14}$$

If $C_o^+ = 0$, then

$$E_{sp}(0) = E_o(\infty) = \max_{\underline{P}} -\ln \left(\sum_j \prod_k p_{j,k}^{P_k} \right) \tag{1.15}$$

The expurgated bound $E_{exp}(R)$ is given by another, more complicated expression. At

zero rate, its value is given by

$$E_{exp}(0) = \max_{\underline{P}} \sum_i \sum_k P_i P_k \left(-\ln \sum_j p_{j,k}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}} \right) \tag{1.16}$$

Attacking the large difference between $E_{exp}(R)$ and $E_{sp}(R)$ for low rates, Shannon and Gallager (1965) have recently found a new, improved upper bound on exponents. Their result states that if one has any arbitrary upper bound on E(R) given by $E_{arb}(R)$, which is tighter (i.e. lower) than $E_{sp}(R)$ for small rates (or even for the single rate R = 0), then one can extend this bound along a straight line E_{SG}, tangent to both E_{arb} and E_{sp}. Similarly for channels with feedback, if one has an arbitrary upper bound on F(R) given by $F_{arb}(R)$, then one can extend this bound along the Shannon-Gallager line $F_{SG}(R)$, tangent to both $F_{arb}(R)$ and $E_{sp}(R)$. (Recall that the sphere packing bound applies to both E(R) and F(R).)

For certain special channels, such as the binary symmetric channel, there are known low-rate upper bounds on exponent, such as the Elias (See Gramenopoulos, 1962) bound, from which the Shannon-Gallager bound can be extended. For most channels, however, no such upper bound at low rates was previously known, either with or without feedback.

The exponents E_M were first implicitly studied by Plotkin (1951) for the binary symmetric channel. More recently, Dobrushin (1962) has computed E_M for a larger class of symmetric binary channels. The nonsymmetric channels pose additional difficulties, however, which have prevented previous computation of E_M. Finally, the exponents F_M have not previously been studied at all, even for the binary symmetric channel.

Using a sequential transmission procedure for the binary symmetric channel with noiseless feedback, M. Horstein(1963) was able to demonstrate significant exponential improvement over normal block coding without feedback. However, it was not clear what part of his improvement resulted from the sequential transmission procedure and what part resulted from the use of feedback. Prior to this thesis there have been no conclusive studies of the limitations of block coding with feedback.

For $R > R_{crit}$, it is known that $E(R) = F(R)$. It can further be shown that, at the other extreme, $E_2 = F_2$. This leads one to wonder whether the error probability using feedback is ever exponentially better than the corresponding one-way system. Another important question concerns the simplicity of coding with feedback. For the binary erasure channel, it is apparent that coding with feedback is quite simple: one need only repeat each bit until it is received unerased. For certain multi-level channels, S. S. L. Chang (1956) has demonstrated conceptually simple coding schemes which achieve an exponentially decaying probability of error, but the resulting exponents are inferior even to those attainable by one-way procedures using random coding. Can one find explicit feedback coding schemes for the binary symmetric channel? Can they be used to attain exponentially optimum error probabilities?

GOALS

The two major objectives of this thesis are to tighten the upper bounds on exponents for block coding, both with and without feedback, and to examine various feedback strategies in relation to these bounds. The upper bounds are tightened by deriving new general low rate results from which the new Shannon-Gallager line can be extended. Particular attention is given to E_∞ and F_∞, which serve as convenient upper bounds on E(0) and F(0). Although certain basic properties of good feedback

strategies are demonstrated in general, the actual construction of asymptotically optimum feedback strategies is restricted to the binary symmetric channel.

It is conceded at the outset that a model which assumes unlimited, delayless, error-free feedback does not realistically apply to most physical communication systems. Nevertheless, the study of this case is interesting from a theoretical viewpoint. It provides an interesting comparison with the normal one-way situation, and between these two extremes one might interpolate these results to find bounds on the performance possible with limited, delayed, noisy feedback loops.

A more promising area for the direct application of some of the results of this thesis is in the statistical design of experiments, a mathematical subject which is isomorphic to the theory of error correcting codes, although the terminology is quite different. The only real difference between these two disciplines is their point of view. Coding theory, following Shannon, tends to emphasize mainly the asymptotic results; the design of experiments, descended from the study of Steiner triple systems and Latin Squares, tends to be concerned almost entirely with questions of the existence and construction of particular fixed composition codes (called "incomplete balanced block designs") of certain block lengths having certain specified distance properties.

The applications of the two subjects are also different. "Codes" are constructed to correct errors expected in the transmission of information over noisy channels; "block designs" are constructed to equalize the anomalous effects expected in the results of a set of noisy experiments (often psychological experiments). In the latter application, it is usually possible to modify subsequent experiments according to the known outcomes of previous experiments, i.e., to make use of the unlimited, delayless, noiseless feedback. Yet prior to this thesis, most of the research in the statistical

design of experiments, as well as in error correcting codes, has been concerned only with one-way situations.

For example, one may wish to determine which of M suspected dietary ingredients (e.g., various cholesterols, sugars, ...) is the primary cause of a particular fatal disease (e.g., heart attacks). There are N animals, each of which is to be placed on a particular lifetime diet containing only some subset of the M suspected ingredients. Which sets of diets will most conclusively reveal the guilty food? One can consider this as a coding problem for a binary asymmetric channel with the inputs indicating presence or absence of the dietary ingredient, and the outputs specifying death due to the disease or to other causes. If all of the N animals are tc be tested simultaneously, we have a one-way coding problem; if they are to be tested sequentially (as might be possible with short-lived animals) with each diet modified according to the outcomes of the previous tests, we have a feedback coding problem.

Like most practical examples, this illustration suffers from several objections: there might be several guilty foods (more than one selected message), and the probabilities relating the incidence of the disease to the diets (the channel probabilities) are imprecisely known. Nevertheless, the theoretical results obtained from an analysis of the abstract problem might well prove helpful to the wise experimenter who tempers his applications of the theory with common sense.

Following the educational biases of this author and his committee, this thesis is written in the language of coding theory. For further discussion of block designs, the interested reader is referred to Bose(1947), Hall(1958), Mann(1949) and Ryser (1963).

Chapter 2

ZERO RATE EXPONENTS FOR ONE-WAY CHANNELS

Chapter Abstract

In this chapter we examine the behavior of E_M, the error exponent for M codewords, for one-way discrete memoryless channels. For a large class of "pairwise reversible" channels, which satisfy

$$\sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}} \ln p_{j,i} = \sum_j p_{j,k}^{\frac{1}{2}} p_{j,i}^{\frac{1}{2}} \ln p_{j,k}$$

for all input pairs (a_i, a_k), we obtain an exact expression for E_M which descends to $E_{exp}(0)$ hyperbolically with increasing M. This expression also serves as a general lower bound on E_M for nonsymmetric channels. Finally, we derive a general upper bound on E_M. Although this bound is often weak for finite M, it proves sufficient to establish the general result, $E_\infty = E_{exp}(0)$.

As an example of the usefulness of this result, we compute E_∞ for Reiffen's (1963) very noisy channel. We find that $E_\infty = R_{comp}$, thus obtaining upper and lower bounds on E(R) which coincide at all rates for very noisy channels.

A revised version of this chapter, together with the derivation of the new Shannon-Gallager line (Figure 1-3), will probably appear in a forthcoming PGIT paper (Shannon, Gallager, & Berlekamp, 1965).

Definitions:

$$E_M = \lim_{N \to \infty} -1/N \ln P_e \tag{2.01}$$

where P_e is the probability of error of the best code with block length N and M equiprobable codewords.

$\Pr(\underline{x} \leftrightarrow \underline{x}') = \Pr(\underline{x}' \leftrightarrow \underline{x})$ is the probability of confusing $\underline{x}$ and $\underline{x}'$,

Pr(decoder selects $\underline{x}'/\underline{x}$ sent) + Pr(decoder selects $\underline{x}/\underline{x}'$ sent)

We first observe that the probability of error for any code of M equiprobable codewords is given by

$$P_e = 1/2M \sum_{\underline{x} \neq \underline{x}'} \sum \Pr(\underline{x} \leftrightarrow \underline{x}') \tag{2.02}$$

There are only M(M-1) terms in this sum. Since M(M-1) remains fixed while N goes to infinity, it is clear that the worst pair alone determines E_M.

$$E_M = \lim_{N \to \infty} \min_{\underline{x}, \underline{x}'} - 1/N \ln \Pr(\underline{x} \leftrightarrow \underline{x}') \tag{2.03}$$

Since (2.03) holds for all M, it is also valid for E_∞.

An asymptotic expression for the error exponent between two given codewords, $\underline{x}$ and $\underline{x}'$, of very large block length, N, follows directly from a theorem of Gallager(1965)

$$\lim_{N \to \infty} -1/N \ln \Pr(\underline{x} \leftrightarrow \underline{x}') = \lim_{N \to \infty} 1/N \; \text{l.u.b.}_{0<s<1} - \sum_i \sum_k N_{i,k} \ln \sum_j p_{j,i}^s \, p_{j,k}^{1-s} \; \dagger \tag{2.04}$$

where $N_{i,k}$ is the number of times a_i occurs in $\underline{x}$ opposite a_k in $\underline{x}'$. $\sum_i \sum_k N_{i,k} = N$. It is convenient to introduce the function

$$u_{i,k}(s) = -\ln \sum_j p_{j,i}^s \, p_{j,k}^{1-s} \tag{2.05}$$

Graphs of this function for certain input pairs of certain channels are plotted in Figs. 2-1 through 2-6. Notice that $u_{k,i}(s) = u_{i,k}(1-s)$. If a_i and a_k have no common output, then $u_{i,k}(s) = \infty$. If this happens for any pair (a_i, a_k), the channel has a zero error capacity, C_o, as introduced by Shannon (1956), and C_o satisfies

---

† l.u.b. means least upper bound.

THE FUNCTION $u_{1,2}(\varepsilon)$ FOR SEVERAL CHANNELS

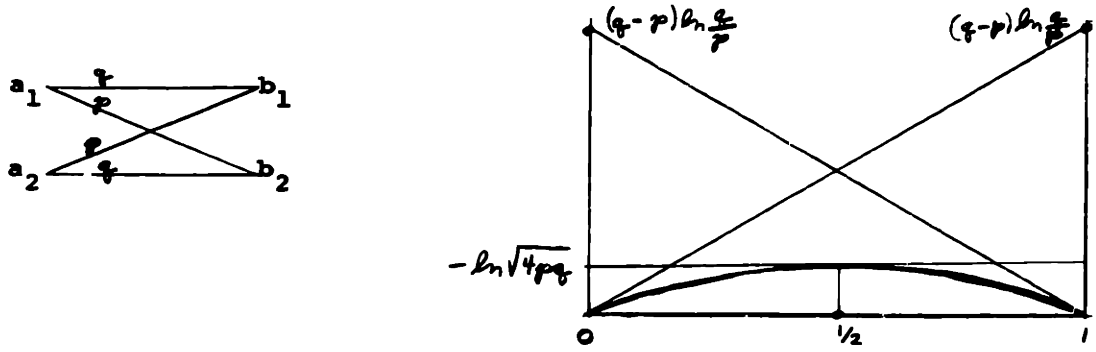


Figure 2-1. The Binary Symmetric Channel (BSC)

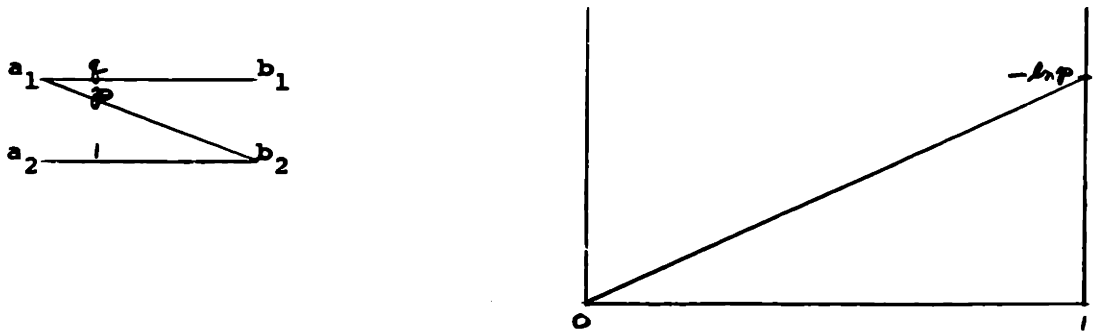


Figure 2-2. The Completely Asymmetric Binary Channel

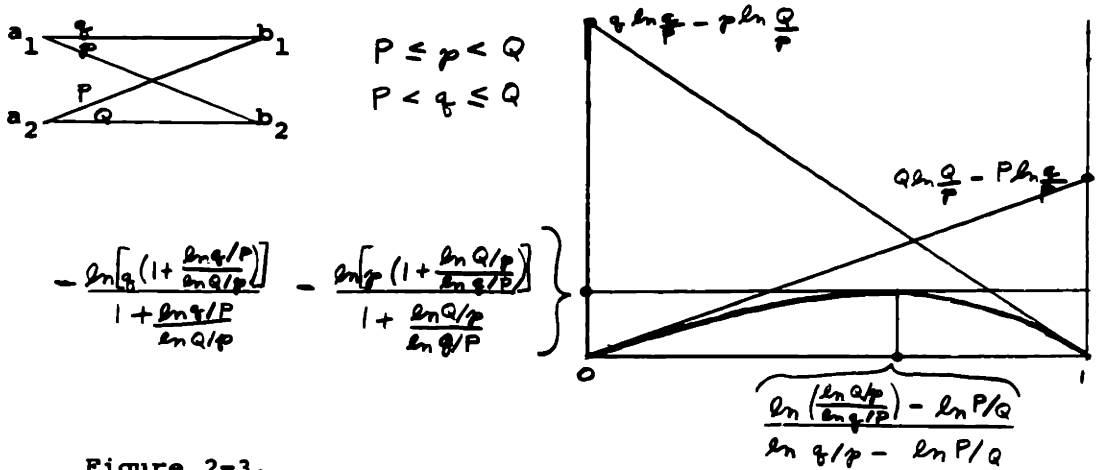


Figure 2-3. The General Asymmetric Binary Channel

THE FUNCTION $u_{1,2}(s)$ FOR SEVERAL CHANNELS

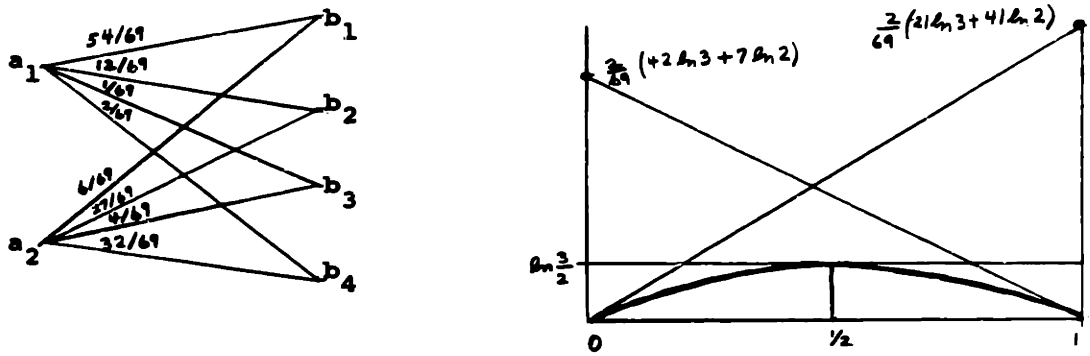


Figure 2-4. A Pairwise Reversible Binary Input Channel

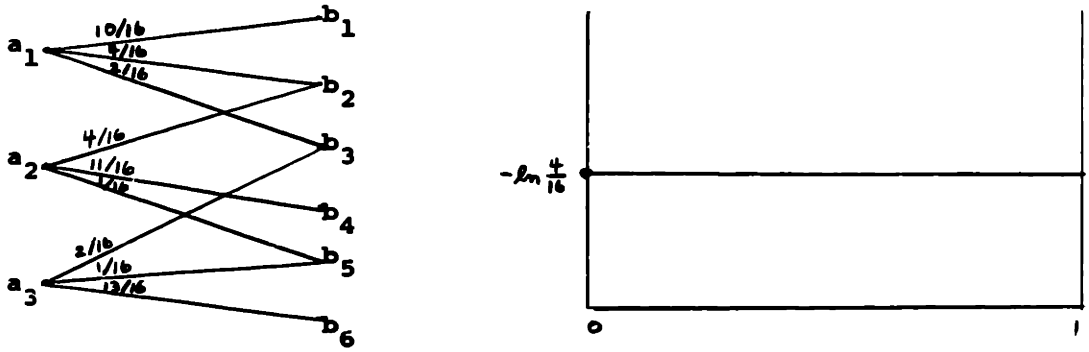


Figure 2-5. A Pairwise Erasing Ternary Input Channel
(non-uniform but pairwise reversible)

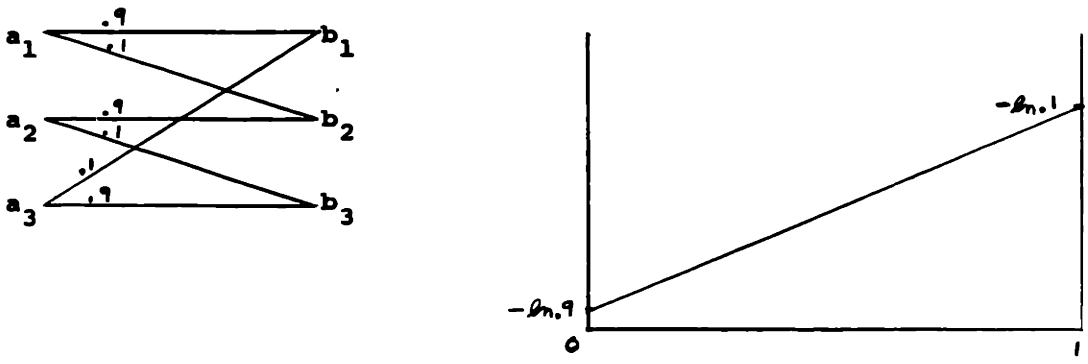


Figure 2-6. A Ternary Unilateral Channel (TUC)
(uniform but not pairwise reversible)

$C_o \geq 1$ bit. On such channels it is possible to transmit at any rate $R \leq C_o$ with a probability of error that is identically zero. Since the exponents E_M are not finite, we exclude such channels from further consideration.

If the channel has no zero error capacity, then $u_{i,k}(s)$ is defined for all pairs (a_i, a_k). For $0 < s < 1$, $u_{i,k}(s) > 0$, except in the degenerate case that $p_{j,i} = p_{j,k}$ for all j, which we may remove from further consideration by combining the identical inputs a_i and a_k.

If the inputs a_i and a_k lead to the same set of channel outputs with nonzero probabilities, then $u_{i,k}(s)$ is continuously differentiable over the closed interval $0 \leq s \leq 1$, with

$$u'_{i,k}(s) = \left(\sum_j p_{j,i}^s \; p_{j,k}^{1-s} \ln (p_{j,k}/p_{j,i}) \right) / \left(\sum_j p_{j,i}^s \; p_{j,k}^{1-s} \right) \qquad (2.055)$$

Some channels, such as the binary erasure channel and the completely asymmetric binary channel shown in Fig. 2-2, do not satisfy this condition for some pairs of inputs. For such channels $u_{i,k}(s)$ and $u'_{i,k}(s)$ may not be well-defined at s=0 or s=1. We remove these ambiguities by setting $u_{i,k}(0) = \lim_{s \to 0^+} u_{i,k}(s)$; $u'_{i,k}(0) = \lim_{s \to 0^+} u'_{i,k}(s)$; and $u_{i,k}(1) = \lim_{s \to 1^-} u_{i,k}(s)$; $u'_{i,k}(1) = \lim_{s \to 1^-} u'_{i,k}(s)$. The function $u_{i,k}(s)$ is then convex upward and continuously differentiable over the closed interval $0 \leq s \leq 1$. We may then replace the least upper bound of (2.04) by a maximum and define an "error exponent" between the two codewords $\underline{x}$ and $\underline{x}'$ by

$$E(\underline{x}, \underline{x}') = 1/N \max_{0<s<1} \sum_i \sum_k N_{i,k} \, u_{i,k}(s) \qquad (2.06)$$

(2.04) assures us that this exponent is asymptotically correct; (2.03) assures us that this exponent, for the worst pair of codewords, determines E_M.

The maximum of the sum on the right hand side of (2.06) cannot excede the sum of the maximums, so

$$E(\underline{x}, x') \leq 1/N \sum_i \sum_k N_{i,k} \max_{0 \leq s \leq 1} u_{i,k}(s) \tag{2.07}$$

with equality iff the same value of s simultaneously maximizes all $u_{i,k}(s)$ for which $N_{i,k} > 0$. If M = 2, then we clearly do best to set $N_{i,k} = N$ for the best pair of inputs (a_i, a_k), and all other $N_{i',k'} = 0$. This gives

$$E_2 = \max_{i,k} \max_{0 \leq s \leq 1} u_{i,k}(s) \tag{2.08}$$

It is interesting to compare this expression for E_2 with $E_{sp}(0)$, the sphere packing bound at zero rate, as given by Gallager (1965).

$$E_{sp}(0) = \max_{\underline{P}} -\ln \sum_j \prod_k (p_{j,k})^{P_k} \tag{1.15}$$

It is apparent that $E_2 \leq E_{sp}(0)$, with equality iff $\underline{P}^*$, the value of $\underline{P}$ which maximizes the expression for $E_{sp}(0)$, has only two nonzero components.

Having found the best pair of inputs for E_2, (a_i, a_k), it clearly does not matter whether we set $N_{i,k} = N$ or $N_{k,i} = N$. However, we must <u>not</u> attempt to form some linear combination of these two optimum solutions, for by making both $N_{i,k}$ and $N_{k,i}$ nonzero we may violate the condition for equality in (2.07). For example, suppose we choose a two-word code for the completely asymmetric binary channel of Fig. 2-2 by setting $N_{i,k} = N_{k,i} = N/2$. The disastrous result is depicted below:

Code 1: $\underline{x}_1 = a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1 a_1$

$\underline{x}_2 = a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2 a_2$

Code 2: $\underline{x}_1 = a_1a_1a_1a_1a_1a_1a_1a_1a_1a_1a_1a_1a_1a_2a_2a_2a_2a_2a_2a_2a_2a_2a_2a_2$

$\underline{x}_2 = a_2a_2a_2a_2a_2a_2a_2a_2a_2a_2a_2a_2a_2a_1a_1a_1a_1a_1a_1a_1a_1a_1a_1a_1$

Using either code, an error will occur only if the received sequence consists entirely of b_1's. For Code 1, $E(\underline{x}_1, \underline{x}_2) = -\ln p$; for Code 2, $E(\underline{x}_i, \underline{x}_2) = -1/2 \ln p$.

If both $N_{i,k}$ and $N_{k,i}$ are nonzero, then there can be equality in (2.07) only if the same value of s maximizes both $u_{i,k}(s)$ and $u_{k,i}(s) = u_{i,k}(1-s)$. If there is a value of s which does this, it is given by $s = 1/2$. This works iff $u'_{i,k}(1/2) = 0$. Since $u_{i,k}(s)$ is convex upward, any stationary point is a global maximum. Carrying out the differentiation gives the condition

$$\sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}} \ln p_{j,i} = \sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}} \ln p_{j,k} \qquad (2.09)$$

If (2.09) holds for some pair of inputs (a_i, a_k), then it is permissible to reverse the order of the symbols a_i and a_k between two codewords (as was done above) without changing the error exponent between the two words. If (2.09) holds for all pairs of channel inputs, a_i and a_k, the channel is said to be pairwise reversible. The class of pairwise reversible channels includes all of the symmetric binary input channels considered by Dobrushin (1962) (which are defined in a manner that guarantees that $u_{i,k}(s) = u_{k,i}(s)$ for all s), and many other binary input channels, such as the one in Fig. 2-4 (as the reader is invited to verify). For multi-input channels, there is no relationship between the class of pairwise reversible channels and the uniform channels discussed by Fano (1961), p. 126). The channel of Fig. 2-5 is pairwise reversible but nonuniform; from any pair of inputs it looks like a binary erasure channel. The channel of Fig. 2-6 is not pairwise reversible even though it is uniform; from any pair of inputs

it looks like an asymmetric binary erasure channel.

For a pairwise reversible channel, the error exponent between two codewords is given by

$$E(\underline{x}, \underline{x}') = 1/N \sum_i \sum_k N_{i,k} u_{i,k}(1/2) \tag{2.10}$$

Since $u_{i,k}(1/2) = u_{k,i}(1/2)$, we are able to define a symmetric "distance" between the pair of inputs (a_i, a_k) by

$$d_{i,k} = d_{k,i} = u_{i,k}(1/2) = -\ln \sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}} \tag{2.11}$$

The distance between the two codewords $\underline{x}_m$ and $\underline{x}_{m'}$ is

$$D(\underline{x}_m, \underline{x}_{m'}) = \sum_i \sum_k N_{i,k}^{(m,m')} d_{i,k} \tag{2.12}$$

Notice that $d_{i,i} = 0$; $D(\underline{x}_m, \underline{x}_m) = 0$.

The distance is asymptotically the logarithm of the probability of error between these two words. According to (2.03), the error exponent over the whole code of M codewords is given by the minimum distance between any two codewords.

$$E_M = \lim_{N \to \infty} 1/N \, D_{min} \tag{2.13}$$

where

$$D_{min} = \min_{m \neq m'} D(\underline{x}_m, \underline{x}_{m'}) \tag{2.14}$$

Proceeding in the manner first introduced by Plotkin (1951) for the binary symmetric channel, we note that the minimum distance cannot excede the average distance.

$$D_{min} \leq 1/(M(M-1)) \sum_m \sum_{m'} D(\underline{x}_m, \underline{x}_{m'}) \tag{2.15}$$

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

$$\sum_{m=1}^{M}\sum_{m'=1}^{M} D(\underset{\sim}{x}_m, \underset{\sim}{x}_{m'}) = \sum_{n=1}^{N}\sum_{i=1}^{K}\sum_{k=1}^{K} M_i(n)M_k(n)\, d_{i,k} \tag{2.16}$$

where $M_k(n)$ is the number of times a_k occurs in the n^{th} column. Let M_k^* denote the number of times a_k occurs in the best possible column,

$$\max_{\Sigma M_k = M} \sum_i \sum_k M_i M_k d_{i,k} = \sum_i \sum_k M_i^* M_k^* d_{i,k} \tag{2.17}$$

Combining (2.13) through (2.17) results in a bound for pairwise reversible channels.

$$E_M \leq 1/(M(M-1)) \sum_i \sum_k M_i^* M_k^* d_{i,k} \tag{2.18}$$

We now show that this bound can always be achieved. To do this, we select the first column of the code so that it has the prescribed composition, a_k occurring M_k^* times. Then we choose as subsequent columns of the code all possible permutations of the first column. The number of columns is given by $N = M!/\pi_k M_k^*!$. If a larger block length is desired, we can repeat the whole code as many times as desired. This enables us to obtain the arbitrarily large block lengths required by the limit in (2.13).

In the constructed code, every column contributes the same maximum amount to the total distance, assuring equality between (2.16) and N times (2.17). Every pair of codewords is the same distance apart, assuring equality in (2.15). Because of these two facts, (2.18) holds with equality.

This construction can likewise be used for channels that are not pairwise symmetric. The constructed code has the property that $N_{i,k}^{(m,m')} = N_{k,i}^{(m,m')} = N_{i,k}$ independent of m and m′. This guarantees that, for this code, (2.06) is maximized by setting s=1/2,

for $u_{i,k}(s) + u_{k,i}(s)$ always attains its maximum at $s = 1/2$, even when $u_{i,k}(s)$ does not.

However, it is often possible to improve this exponent for channels which are not pairwise reversible by choosing $N_{i,k} \neq N_{k,i}$, as we have seen. We summarize these results in a theorem.

Theorem:

$$E_M \geq 1/(M(M-1)) \max_{\Sigma M_k = M} \Sigma\Sigma_{i\ k} M_i M_k (-\ln \Sigma_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}}) \tag{2.2}$$

with equality for channels which are pairwise reversible.

We next compare this result with $E_{exp}(0)$, Gallager's (1964) lower bound to E(0), the error exponent at infinitesmal rates. $E_{exp}(0)$ is given by Gallager as

$$E_{exp}(0) = \max_{\underline{P}} \Sigma\Sigma_{i\ k} P_i P_k (-\ln \Sigma_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}}) \tag{1.16}$$

$\underline{P}$ is the probability vector specifying the composition of the code. The vector $\underline{P}$ is unrestricted by the Diophontine constraints placed on the vector $\underline{M}^*/M$ (M_k^* is the k^{th} component of $\underline{M}^*$). This additional freedom can only improve $E_{exp}(0)$. This proves the first of the two corollaries.

Corollary 1: For pairwise reversible channels,

$$E_M \leq (M/(M-1)) \quad E_{exp}(0) \tag{2.201}$$

Corollary 2: For any channel,

$$E_M \geq (M/(M-1))\, E_{exp}(0) - (1/4M(M-1))\, (K u_{min} + \Sigma\Sigma_{i \neq k} (u_{i,k}(1/2) - u_{min})) \tag{2.202}$$

where K is the number of channel inputs and

$$u_{min} = \min_{i \neq k} u_{i,k} \quad (1/2) \tag{2.203}$$

Proof: In this proof, we let $[x]$ denote the greatest integer less than or equal to x; $[x]^+$, the least integer greater than x. $[x]^+ = [x] + 1$.

$\underline{P}^*$ is the vector which optimizes the expression for $E_{exp}(0)$.

Let Z be the number of k's for which $P_k^* = 0$. Z is an integer, $0 \leq Z \leq K-2$.

Let $A = \sum_k ([MP_k^*]^+ - MP_k^*)$ (2.204)

A is an integer; $0 \leq A \leq K - Z$

Now let δ_{max} be the value of the A^{th} largest $([MP_k^*]^+ - MP_k^*)$.

Define $\underline{M}$ by

$M_k = 0$ if $P_k^* = 0$

$M_k = [MP_k^*]$ for A different k's, each of which has

$$\delta_{max} \leq ([MP_k^*]^+ - MP_k^*) \leq 1$$

$M_k = [MP_k^*]^+$ for the other (K-A-Z) k's, each of which has

$$0 \leq ([MP_k^*]^+ - MP_k^*) \leq \delta_{max} \quad . \tag{2.205}$$

The vector $\underline{M}$ then satisfies

$$\sum_k M_k = \sum_k [MP_k^*]^+ - A = M \tag{2.206}$$

$$M_k = 0 \text{ if } P_k^* = 0 \tag{2.207}$$

$$(\delta_{max} - 1) \leq (M_k - MP_k^*) \leq \delta_{max} \tag{2.208}$$

Define $\delta_k = M_k - MP_k^*$; $\delta_o = \delta_{max} - 1/2$ (2.209)

Notice that $\sum_k \delta_k = 0$; $\delta_k = 0$ if $P_k^* = 0$; (2.210)

and $|\delta_k - \delta_o| \leq 1/2$. (2.211)

Then from Theorem 2.2

$$M(M-1)\, E_M \geq \sum_i \sum_k M_i M_k u_{i,k}(1/2) \tag{2.212}$$

$$\begin{aligned} M(M-1)\, E_M - M^2 E_{exp}(0) &\geq \sum_i \sum_k (M_i M_k - M^2 P_i^* P_k^*)\, u_{i,k}(1/2) \\ &= \sum_i \sum_k (\delta_i \delta_k + M P_i^* \delta_k + M P_k^* \delta_i)\, u_{i,k}(1/2) \end{aligned} \tag{2.213}$$

We can discard the two latter terms on the right by invoking the fact that the probability vector $\underline{P}^*$ maximizes the expression for $E_{exp}(0)$. Using the LaGrange multiplier λ, we define

$$f(\underline{P}) = \sum_i \sum_k P_i P_k u_{i,k}(1/2) - \lambda \left(\sum_k P_k - 1\right) \tag{2.220}$$

According to well-known results of mathematical programming,

$$\max_{\underline{P}} f(\underline{P}) = f(\underline{P}^*) \text{ only if}$$

$$\left[\frac{\partial f}{\partial P_h}\right]_{\underline{P} = \underline{P}^*} \leq 0 \text{ with equality unless } P_h^* = 0 \tag{2.221}$$

Computing the derivative gives

$$\begin{aligned} \frac{\partial f}{\partial P_h} &= \sum_k P_k u_{h,k}(1/2) + \sum_i P_i u_{i,h}(1/2) - \lambda \\ &= 2 \sum_k P_k u_{h,k}(1/2) - \lambda \end{aligned} \tag{2.222}$$

Hence

$$\sum_k P_k^* u_{i,k}(1/2) \leq \lambda/2, \text{ with equality unless } P_i^* = 0. \tag{2.223}$$

Recalling (2.210), we have

$$\sum_i \sum_k \delta_i P_k^* u_{i,k}(1/2) = 0 \tag{2.224}$$

Applying this to (2.213) gives

$$M(M-1)\, E_M - M^2 E_{exp}(0) \geq \sum_{i \neq k} \sum \delta_i \delta_k u_{i,k}(1/2) \tag{2.225}$$

$$= u_{min} \sum_{i \neq k} \sum \delta_i \delta_k + \sum_{i \neq k} \sum \delta_i \delta_k (u_{i,k}(1/2) - u_{min}) \tag{2.226}$$

where $u_{min} = \min_{i \neq k} u_{i,k}(1/2)$ (2.227)

For the first term,

$$0 = \left(\sum_k \delta_k \right)^2 = \sum_k \delta_k^2 + \sum_{i \neq k} \sum \delta_i \delta_k \tag{2.230}$$

$$\sum_{i \neq k} \sum \delta_i \delta_k = - \sum_k \delta_k^2 = - \sum_k (\delta_k - \delta_o + \delta_o)^2 \tag{2.231}$$

$$= - \sum_k (\delta_k - \delta_o)^2 + K \delta_o^2 \tag{2.232}$$

$$\geq - \sum_k (\delta_k - \delta_o)^2 \tag{2.233}$$

$$\geq - K/4 \text{ by } 2.211 \tag{2.234}$$

For the second term, by (2.208) and (2.209), if $\delta_i \delta_k < 0$, then

$$\delta_i \delta_k \geq \delta_{max}(\delta_{max-1}) = (\delta_o + 1/2)(\delta_o - 1/2) \geq -1/4 \tag{2.236}$$

So $\delta_i \delta_k \geq -1/4$. (2.237)

Substituting (2.237) and (2.234) into (2.226) yields the corollary. Q.E.D.

Certain other corollaries of this type may be proved using the methods of Niven (1963).

Corollary 2 holds with equality for channels which are both pairwise reversible and pairwise uniform ($u_{i,k}(1/2) = u_{min}$ for all pairs $i \neq k$)† if K is even and M is a multiple of K/2 but not of K. For channels which are pairwise very uniform, one can often obtain a tighter bound by applying (2.225) directly to the particular channel or by a different choice of the vector $\underline{M}$ than the one defined by equations (2.205)

Dobrushin (1962) computed E_M for a class of "symmetric binary input channels" (for which $u_{1,2}(s) = u_{2,1}(s)$). His results show that for such channels, Corollary 1 holds with equality if M is even, while Corollary 2 holds with equality if M is odd. It is readily seen this is also true under the weaker assumption that $u'_{1,2}(1/2) = 0$, as stated in (2.09).

We now proceed to derive a general upper bound on E_M. Although our argument is carried out in the general case, we will make frequent references to the ternary unilateral channel of Fig. 2-6. The reader is advised to keep this concrete example in mind throughout the discussion.

Since we are interested primarily in showing that $E_\infty = E_{exp}(0)$, we start with an assumed too-good code having a very large number of codewords and an even larger block length. Our first step is to define a relationship of dominance over pairs of codewords.

† Examples of such channels are given in Exercise 2-1(Upper bound) at the end of this chapter. Pairwise reversibility cinches equality in Theorem 2.2; pairwise uniformity eliminates the second term in (2.226). For such channels, $P_k^* = 1/K$. If K is even and M is a multiple of K/2 but not of K, then $\delta_k = \pm 1/2$; and $\delta_o = 0$, giving equality in (2.233) and (2.234).

Definition: $\underline{x}_m$ dominates $\underline{x}_{m'}$ iff

$$\sum_i \sum_k N_{i,k}^{(m,m')} u'_{i,k}(1/2) \geq 0 \tag{2.30}$$

Notice that either $\underline{x}_m$ dominates $\underline{x}_{m'}$, or $\underline{x}_{m'}$ dominates $\underline{x}_m$, or both, because

$$N_{i,k}^{(m,m')} = N_{k,i}^{(m',m)} ; \quad u'_{i,k}(1/2) = -u'_{k,i}(1/2)$$

so

$$\sum_i \sum_k N_{i,k}^{(m',m)} u'_{i,k}(1/2) = - \sum_i \sum_k N_{i,k}^{(m,m')} u'_{i,k}(1/2) \tag{2.31}$$

For the TUC the codeword consisting of all a_1's dominates any other codeword which contains at least as many a_2's as a_3's, but it is dominated by any other codeword which contains at least as many a_3's as a_2's.

Notice that dominance is not transitive except when $K = 2$ and the input alphabet is binary. In general, we may have $\underline{x}$ dominate $\underline{x}'$ and $\underline{x}'$ dominate $\underline{x}''$ without having $\underline{x}$ dominate $\underline{x}''$.

Lemma: If $\underline{x}_m$ dominates $\underline{x}_{m'}$, then

$$E(\underline{x}_m, \underline{x}_{m'}) \leq 1/N \sum_i \sum_k N_{i,k}^{(m,m')} (u_{i,k}(1/2) + 1/2\, u'_{i,k}(1/2)) \tag{2.32}$$

Proof: Recall from (2.05) that

$$E(\underline{x}, \underline{x}') = 1/N \max_{0 \leq s \leq 1} \sum_i \sum_k N_{i,k} u_{i,k}(s) \tag{2.33}$$

The tangent line to a convex upward function is an upper bound on the function. Taking this tangent at $s = 1/2$ overbounds $E(\underline{x}_m, \underline{x}_{m'})$.

$$E(\underline{x}_m, \underline{x}_{m'}) \leq 1/N \max_{0 \leq s \leq 1} \sum_i \sum_k N_{i,k}^{(m,m')} (u_{i,k}(1/2) + (s-1/2) u'_{i,k}(1/2)). \tag{2.34}$$

From (2.30), this linear function of s is maximized at $s^* = 1$. Q.E.D.

We now proceed to extract from our original code of M codewords a certain subset of at least log M codewords which form an "ordered" code, in which each word dominates every subsequent word. This is accomplished in the following manner: We first find the word in the original code which dominates the most others. This word must dominate at least half of the other words. We select that word as $\underline{x}_1$ in the ordered code. All words in the original code which are not dominated by $\underline{x}_1$ are then discarded. From the remaining words in the original code, we select the word which dominates the most others and choose it as $\underline{x}_2$ in the ordered code. The words which are not dominated by $\underline{x}_2$ are then discarded from the original code. This process is continued until all words of the original code are either placed in the ordered code or discarded. Since no more than half of the remaining words in the original code are discarded as each new word is placed in the ordered code, the ordered code contains at least log M codewords.

Within the ordered code, for any $1 \leq m < m' \leq \log M$ we now have

$$E(\underline{x}_m, \underline{x}_{m'}) \leq 1/N \sum_i \sum_k N_{i,k}^{(m,m')} (u_{i,k}(1/2) + 1/2\, u'_{i,k}(1/2)) \tag{2.35}$$

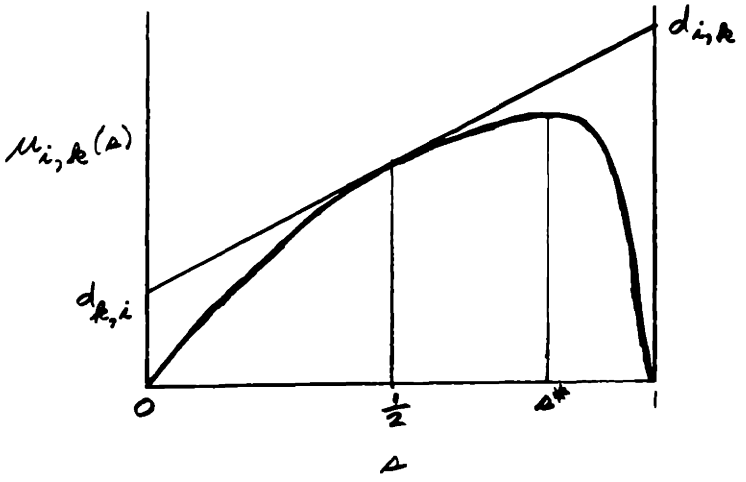
We define the asymmetric "distances"

$$d_{i,k} = u_{i,k}(1/2) + 1/2\, u'_{i,k}(1/2) \tag{2.36}$$

A graphic interpretation of $d_{i,k}$ is given in Fig. 2-7. Convexity assures that both $d_{i,k}$ and $d_{k,i}$ are nonnegative. Unless the channel has a positive zero error capacity, all of the $d_{i,k}$ are finite and we may define

$$d_{max} = \max_{i,k} d_{i,k} \tag{2.365}$$

Figure 2-7



Similarly we define the distance between a pair of codewords $\underline{x}_m$ and $\underline{x}_{m'}$ (for $m < m'$)

$$D(\underline{x}_m, \underline{x}_{m'}) = \sum_i \sum_k N_{i,k}^{(m,m')} d_{i,k} \tag{2.37}$$

Substituting (2.36) and (2.37) into (2.35) yields

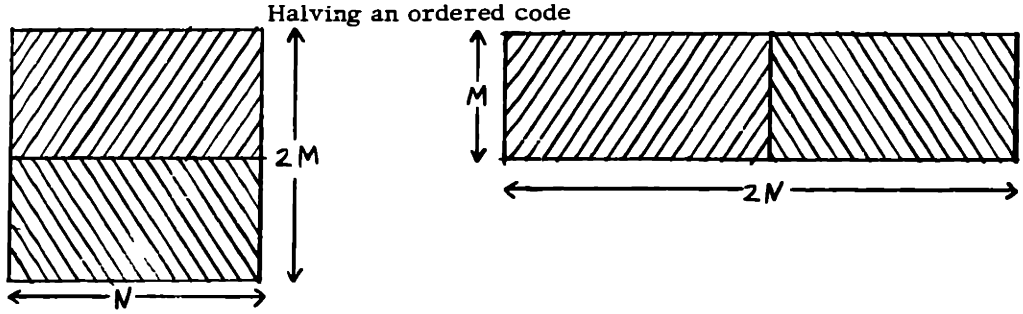
$$E(\underline{x}_m, \underline{x}_{m'}) \leq 1/N \; D(\underline{x}_m, \underline{x}_{m'}) \qquad \text{for } m < m' \text{ in the ordered code.} \tag{2.38}$$

We should now like to invoke the usual Plotkin argument that the minimum distance is less than the average distance, and the average distance can be computed on a

per column basis. Unfortunately, this direct approach does not work because it is possible for many columns to make undeservedly large contributions to the total distance. For example, consider a code for the TUC. A column whose top fourth contains a_1's, whose middle half contains a_2's, and whose bottom fourth contains a_3's contributes $-1/2 \ln 1/10 - 1/8 \ln 9/10$ to the average distance. We wish to show that D_{min}/N, the minimum distance per digit, is actually no better than $-1/3 \ln 1/10 - 1/3 \ln 9/10$. We cannot do this directly because of columns of the type just mentioned. We note, however, that this column which contributes so heavily to the total distance contributes little to distances between words in the same quarter of the block. It happens that all such strange columns have some fatal weakness of this sort, which we exploit by the following construction.

Figure 2-8

Halving an ordered code



Before After

Given an ordered code with 2M words of block length N, we can form an ordered code with M words of block length 2N by annexing the $(M+i)^{th}$ word to the i^{th} word, for all $i = 1, \ldots, M$. The distance from $\underline{x}_m$ to $\underline{x}_{m'}$, $(m < m')$ in the new code is the sum of two distances in the old code, $D(\underline{x}_m, \underline{x}_{m'}) + D(\underline{x}_{m+M}, \underline{x}_{m'+M})$. Any sum of ordered distances in the new code is the sum of twice as many ordered

distances in the old code. The minimum distance of the new code is at least twice the minimum distance of the old code. The minimum distance/digit, D_{min}/N, is not decreased by the halving operation.

We define the probability vector $\underline{p}(n)$, $n = 1, \ldots, N$, as the average composition of the n^{th} column of the old code. The number of a_k's in the n^{th} column is given by $Mp_k(n)$. Likewise we define $\underline{p}'(n)$, $n = 1, \ldots, 2N$,† as the average composition of the n^{th} column of the new code. By the halving construction

$$\underline{p}(n) = 1/2\ (\underline{p}'(n) + \underline{p}'(n+N)) \tag{2.50}$$

We also define

$$\underline{r}(n) = \underline{p}'(n) - \underline{p}(n) \qquad \text{for } n = 1, \ldots, N \tag{2.51}$$

Then for $n = 1, \ldots, N$

$$\underline{p}'(n+N) = \underline{p}(n) - \underline{r}(n) \tag{2.52}$$

$$\underline{r}(n) = 1/2\ (\underline{p}'(n) - \underline{p}'(n+N)) \tag{2.53}$$

The average composition of either code is given by

$$\bar{\underline{p}} = 1/N \sum_{n=1}^{N} \underline{p}(n) = \bar{\underline{p}}' = 1/2N \sum_{n=1}^{2N} \underline{p}'(n) \tag{2.54}$$

The average variance of the column compositions is defined in the obvious manner, the compositions being treated as vectors and the square being taken as the dot product with itself, $\underline{p}(n)^2 = \sum_k p_k(n)^2$.

† There should be no confusion of $\underline{p}'(n)$ with any undefinable derivative of $\underline{p}$.

$$\mathrm{Var}(\underline{p}) = 1/N \sum_{n=1}^{N} (\underline{p}(n) - \overline{\underline{p}})^2 = (1/N \sum_{n=1}^{N} \underline{p}(n)^2) - \overline{\underline{p}}^2 \tag{2.55}$$

$$\mathrm{Var}(\underline{p}') = 1/2N \sum_{n=1}^{2N} (\underline{p}'(n) - \overline{\underline{p}}')^2 = (1/2N \sum_{n=1}^{2N} \underline{p}'(n)^2) - \overline{\underline{p}}'^2 \tag{2.56}$$

Since

$$0 \le p_k(n) \le 1, \qquad \text{for all } k \text{ and } n \tag{2.565}$$

$$\mathrm{Var}(\underline{p}) < 1 \tag{2.57}$$

$$\Delta V = \mathrm{Var}(\underline{p}') - \mathrm{Var}(\underline{p})$$

$$= 1/N \left(1/2 \sum_{n=1}^{2N} \underline{p}'(n)^2 - \sum_{n=1}^{N} \underline{p}(n)^2\right) \tag{2.58}$$

$$= 1/N \left\{1/2 \sum_{n=1}^{N} (\underline{p}'(n)^2 + \underline{p}'(n+N)^2) - 1/4 \sum_{n=1}^{N} (\underline{p}'(n) + \underline{p}'(n+N))^2\right\} \tag{2.585}$$

$$= 1/N \sum_{n=1}^{N} ((\underline{p}'(n) - \underline{p}'(n+N))/2)^2 \tag{2.59}$$

$$= 1/N \sum_{n=1}^{N} \underline{r}(n)^2 \tag{2.60}$$

$$= 1/N \sum_{n=1}^{N} R(n)^2 \ge 0 \tag{2.61}$$

where we have defined the scalar

$$R(n) = (\underline{r}(n)^2)^{\frac{1}{2}} \tag{2.62}$$

Notice that $0 \le R(n) < 1$, and any component of $\underline{r}(n)$ satisfies

$$r_k(n) \le R(n) < 1. \tag{2.63}$$

Furthermore,

$$\sum_k |r_k| / K \le (\sum |r_k|^2/K)^{\frac{1}{2}} \tag{2.635}$$

because no mean can excede the corresponding root mean square.†

If ΔV is small, then most columns of the old code have essentially the same composition in the top half as in the bottom half. This enables us to bound the average of the M^2 distances from any of the first M codewords to any of the second M codewords. The contribution to this average from the n^{th} column is given by

$$\sum_i \sum_k d_{i,k}\, p'_i(n)\, p'_k(n+N) \tag{2.64}$$

From (2.51) and (2.52) we have

$$p'_i(n)\, p'_k(n+N) = (p_i(n) + r_i(n))\ (p_k(n) - r_k(n)) \tag{2.641}$$

$$= p_i(n)\, p_k(n) + r_i(n)\, p_k(n) - p'_i(n)\, r_k(n) \tag{2.642}$$

---

† This well-known theorem, originally due to Cauchy (1821), can be derived at once by verifying that

$$0 \le \Sigma (K^{\frac{1}{2}} |r_k| - R)^2 = 2RK^{3/2} (RK^{-\frac{1}{2}} - \Sigma |r_k|/K).$$

This is a special case (obtained by setting $q_k = 1/K$) of the theorem of the means, which states that $f(s) = (\Sigma q_k r_k^s)^{1/s}$ is a monotonic nondecreasing function of s for any nonnegative numbers r_k and any probability distribution q. Proof is given by Hardy, Littlewood, and Polya, p. 26. The great generality of this theorem is indicated by the following observations: $f(-\infty) = r_{min}$; f(-1) = harmonic mean; f(0) = geometric mean; f(1) = arithmetic mean; f(2) = root mean square; $f(\infty) = r_{max}$.

$$|p_i'(n)p_k'(n+N) - p_i(n)p_k(n)| = |r_i(n)p_k(n) - p_i'(n)r_k(n)| \tag{2.643}$$

$$\sum_i \sum_k d_{i,k}(|p_i'(n)\,p_k'(n+N) - p_i(n)p_k(n)|) \leq d_{max} \sum_{i \neq k} \sum |r_i(n)p_k(n) - p_i'(n)r_k(n)| \tag{2.644}$$

$$< d_{max} \sum_i \sum_k (|r_i(n)p_k(n)| + |p_i'(n)r_k(n)|) \tag{2.645}$$

$$= 2d_{max} \sum_k |r_k(n)| \tag{2.646}$$

$$\leq 2K^{\frac{1}{2}} d_{max} R(n) \text{ by (2.635)} \tag{2.647}$$

Averaging this over all N columns gives

$$|1/N \sum_{n=1}^{N} \sum_i \sum_k d_{i,k}(p_i'(n)p_k'(n+N) - p_i(n)p_k(n))| < 2K^{\frac{1}{2}} d_{max} \sum_{n=1}^{N} R(n)/N$$

$$\leq 2K^{\frac{1}{2}} d_{max}(\sum_{n=1}^{N} R(n)^2/N)^{\frac{1}{2}} \quad \text{(by Cauchy)}$$

$$= 2K^{\frac{1}{2}} d_{max}(\Delta V)^{\frac{1}{2}} \tag{2.65}$$

We define

$$\epsilon = 2K^{\frac{1}{2}} d_{max}(\Delta V)^{\frac{1}{2}} \tag{2.66}$$

We now compute the desired bound on the minimum distance

$$D_{min}/N \leq 1/N \sum_{m=1}^{M} \sum_{m'=M+1}^{2M} D(\underline{x}_m, \underline{x}_{m'})/M^2 \tag{2.67}$$

$$= 1/N \sum_{n=1}^{N} \sum_i \sum_k d_{i,k}\, p_i'(n)\, p_k'(n+N) \text{ by (2.64)} \tag{2.68}$$

$$< 1/N \sum_{n=1}^{N} \sum_i \sum_k d_{i,k} p_i(n)p_k(n) + \epsilon \tag{2.69}$$

$$= 1/N \sum_{n=1}^{N} 2 \sum\sum_{i<k} 1/2\,(d_{i,k} + d_{k,i}) p_i(n) p_k(n) + \epsilon \tag{2.70}$$

$$= 1/N \sum_{n=1}^{N} 2 \sum\sum_{i<k} p_i(n) p_k(n) \left(-\ln \sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}}\right) + \epsilon \tag{2.71}$$

$$= 1/N \sum_{n=1}^{N} \sum\sum_{i\ k} p_i(n) p_k(n) \left(-\ln \sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}}\right) + \epsilon \tag{2.72}$$

$$\leq \sum\sum_{i\ k} P_i^* P_k^* \left(-\ln \sum_j p_{j,i}^{\frac{1}{2}} p_{j,k}^{\frac{1}{2}}\right) + \epsilon \tag{2.73}$$

$$= E_{exp}(0) + \epsilon \tag{2.74}$$

We now show that for sufficiently large M, ΔV (and consequently ϵ, as given by (2.66)), may be taken as an infinitesmal, ϵ'. The average variance of the column compositions of the original ordered code must be nonnegative. As we halve the code again and again, the variance cannot decrease (2.61). But the variance must always remain less than one (2.57). Consequently, if we halve the code $1/\epsilon'$ times consecutively, at some stage the variance must increase by less than ϵ'. At such a halving, we invoke (2.67) through (2.74).

For given ϵ, we start with an original unordered code containing $M \geq 2^{2^{1/\epsilon'}}$ codewords. The ordering process gives us an ordered code containing $\geq 2^{1/\epsilon'}$ codewords. This code is halved up to $1/\epsilon'$ times, until at some halving $\Delta V < \epsilon'$.

We conclude that if $M \geq 2^{2^{1/\epsilon'}}$, then $E_M < E_{exp}(0) + \epsilon$ or,

$$E_M < E_{exp}(0) + 2K^{\frac{1}{2}} d_{max} / (\log \log M)^{\frac{1}{2}} \tag{2.75}$$

$$E_\infty = E_{exp}(0) . \tag{2.76}$$

Application to Very Noisy Channels

Definition: A channel is "very noisy" if

$$|1-(p_{j,i}/p_{j,k})| \ll 1 \qquad \text{for all } i,j,k \tag{2.801}$$

For any channel, and any given input probability distribution $\underline{P}$, the output probability distribution $\underline{q}$ is defined by

$$q_j = \sum_k P_k p_{j,k} \tag{2.802}$$

We may define $\epsilon_{j,k}$ by

$$p_{j,k} = q_j(1 + \epsilon_{j,k}) \tag{2.803}$$

Straightforward manipulation shows that

$$\sum_j q_j \epsilon_{j,k} = 0 \tag{2.804}$$

$$\sum_k P_k \epsilon_{j,k} = 0 \tag{2.805}$$

For very noisy channels, definition (2.801) implies that for all j,k

$$|\epsilon_{j,k}| \ll 1 \tag{2.806}$$

The concept of a very noisy channel was first introduced by Reiffen (1963) and extended by Gallager (1964). Although conceptually equivalent, our definition (2.801) differs from previous formulations. Definition (2.803) leads to the computationally useful (although not strictly necessary) properties (2.804) and (2.805), which our formulation preserves. Although it follows immediately from (2.801), the necessary property (2.806) cannot itself be taken as a definition, for our $\epsilon_{j,k}$ depend on the channel input

probabilities $\underline{P}$ as well as on the channel transition matrix, $p_{j,k}$.

We may compute the capacity by a straightforward power series expansion in ϵ

$$C = \max_{\underline{P}} \sum_j \sum_k P_k p_{j,k} \ln \left(\frac{p_{j,k}}{q_j} \right) \tag{2.811}$$

$$\ln \left(\frac{p_{j,k}}{q_j} \right) = \ln (1+\epsilon_{j,k}) = \epsilon_{j,k} - \epsilon_{j,k}^2/2 + o(\epsilon^3) \tag{2.812}$$

$$p_{j,k} \ln \left(\frac{p_{j,k}}{q_j} \right) = q_j(1+\epsilon_{j,k}) (\epsilon_{j,k} - \epsilon_{j,k}^2/2 + o(\epsilon^3)) \tag{2.813}$$

$$= q_j(\epsilon_{j,k} + \epsilon_{j,k}^2/2 + p(\epsilon^3)) \tag{2.814}$$

$$C = \max_{\underline{P}} \sum_j \sum_k P_k q_j(\epsilon_{j,k} + \epsilon_{j,k}^2/2 + o(\epsilon^3)) \tag{2.815}$$

$$= \max_{\underline{P}} \frac{1}{2} \sum_j \sum_k P_k q_j \epsilon_{j,k}^2 + o(\epsilon^3) \tag{2.816}$$

Similarly we may compute the entire $E_{rand}(R)$ curve, using Gallager's function $E_o(\rho)$

$$E_o(\rho) = \max_{\underline{P}} -\ln \left[\sum_j \left(\sum_k P_k p_{j,k}^{\frac{1}{1+\rho}} \right)^{1+\rho} \right] \tag{1.10}$$

$$= \max_{\underline{P}} -\ln \left[\sum_j q_j \left(\sum_k P_k (1+\epsilon_{j,k})^{\frac{1}{1+\rho}} \right)^{1+\rho} \right] \tag{2.822}$$

$$(1+\epsilon_{j,k})^{\frac{1}{1+\rho}} = 1 + \frac{\epsilon_{j,k}}{1+\rho} - \frac{\rho}{2(1+\rho)^2} \epsilon_{j,k}^2 + o(\epsilon^3) \tag{2.823}$$

$$\sum_k P_k (1+\epsilon_{j,k})^{\frac{1}{1+\rho}} = 1 - \frac{\rho}{2(1+\rho)^2} \sum_k P_k \epsilon_{j,k}^2 + o(\epsilon^3) \tag{2.824}$$

$$E_o(\rho) = \max_{\underline{P}} -\ln \left[\sum_j q_j \left(1 - \frac{\rho}{2(1+\rho)} \sum_k P_k \epsilon_{j,k}^2 + o(\epsilon^3)\right)\right] \tag{2.825}$$

$$= \max_{\underline{P}} \frac{\rho}{2(1+\rho)} \sum_j \sum_k q_j P_k \epsilon_{j,k}^2 + o(\epsilon^3) = \frac{\rho C}{(1+\rho)} + o(\epsilon^3) \tag{2.826}$$

This shows that the input distribution, $\underline{P}$, which attains capacity is also optimum at all lesser rates $0 \le R \le C$. It follows at once that $C = E_o'(0) = C$, in accord with our previous computation. We also have $R_{comp} = E_o(1) = C/2$, and $R_{crit} = E_o'(0) = C/4$, as was shown by Reiffen (1963) and Gallager (1964). Similarly we may compute E_∞.

$$E_\infty = \max_{\underline{P}} \sum_i \sum_k P_i P_k \left(-\ln \sum_j p_{j,k}^{\frac{1}{2}} p_{j,i}^{\frac{1}{2}} \right) \qquad (1.16) \text{ and } (2.76)$$

$$\sum_j p_{j,k}^{\frac{1}{2}} p_{j,i}^{\frac{1}{2}} = \sum_j q_j (1+\epsilon_{j,k})^{\frac{1}{2}} (1+\epsilon_{j,i})^{\frac{1}{2}} \tag{2.832}$$

$$= \sum_j q_j \left[1 + \frac{1}{2}(\epsilon_{j,k} + \epsilon_{j,i} + \epsilon_{j,k}\epsilon_{j,i}) - \frac{1}{8}(\epsilon_{j,k}^2 + \epsilon_{j,i}^2 + 2\epsilon_{j,k}\epsilon_{j,k}) + o(\epsilon^3)\right] \tag{2.833}$$

$$= 1 + \frac{1}{4} \sum_j q_j \epsilon_{j,k}\epsilon_{j,i} - \frac{1}{8} \sum_j q_j (\epsilon_{j,k}^2 + \epsilon_{j,i}^2) + o(\epsilon^3) \tag{2.834}$$

$$E_\infty = \max_{\underline{P}} \sum_i \sum_k P_i P_k \left[\frac{1}{8} \sum_j q_j (\epsilon_{j,k}^2 + \epsilon_{j,i}^2) - \frac{1}{4} \sum_j q_j \epsilon_{j,k}\epsilon_{j,i} + o(\epsilon^3)\right] \tag{2.836}$$

$$= \max_{\underline{P}} \frac{1}{8} \sum_j q_j \left[\sum_i \sum_k P_i P_k (\epsilon_{j,k}^2 + \epsilon_{j,i}^2) - 2\left(\sum_i P_i \epsilon_{j,i}\right)\left(\sum_k P_k \epsilon_{j,k}\right) + o(\epsilon^3)\right] \tag{2.837}$$

$$= \max_{\underline{P}} \frac{1}{8} \sum_j q_j \, 2 \sum_i \sum_k P_i P_k \epsilon_{j,k}^2 + o(\epsilon^3) \tag{2.838}$$

$$= \max_{\underline{P}} \frac{1}{4} \sum_k \sum_j q_j P_k \epsilon_{j,k}^2 + o(\epsilon^3) \tag{2.839}$$

$$= \frac{1}{2} C + o(\epsilon^3) = R_{comp} + o(\epsilon^3) \tag{2.840}$$

The significance of this result is that, when this expression for E_∞ is used as starting point for the Shannon-Gallager (1965) line which overbounds E(R), the resulting bound coincides with the lower bound to E(R) found by Gallager (1964). Thus, for very noisy channels, the exponent rate curve is completely known, for all rates $0 \leq R \leq C$. Its graph is shown in Figure 2-9.

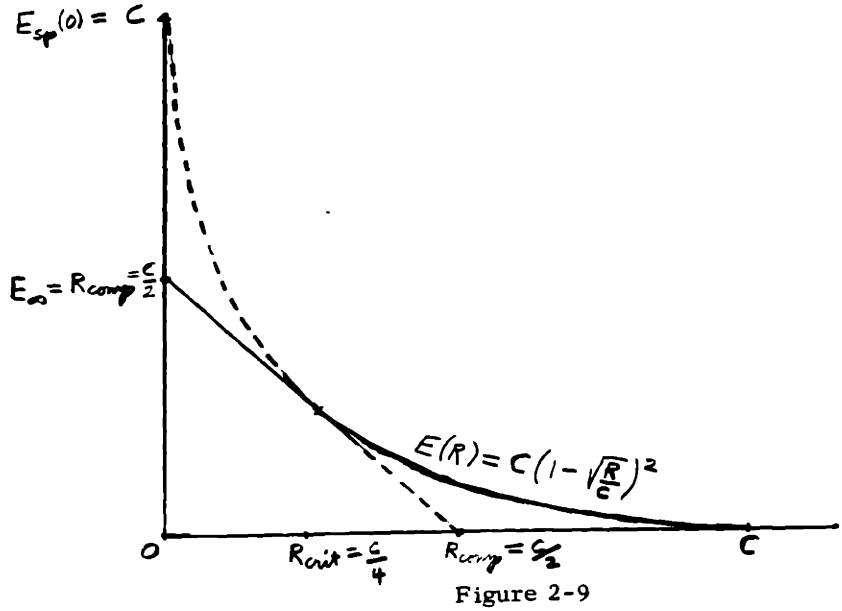


Figure 2-9

E(R) vs R for very noisy channels

Exercises

Exercise 2-1: Prove that $1/4\ E_2 \leq E_\infty \leq (K-1)/K\ E_2$, where K is the number of channel inputs. Give an example of equality at the lower bound. For each K, give an example of equality at the upper bound.

Lower bound solution: Let $E_2 = u_{i^*, k^*}(s^*)$. Set $P_{i^*} = P_{k^*} = 1/2$: $P_k = 0$ for $k^* \neq k \neq i^*$. Then

$$E_\infty \geq \sum_i \sum_k P_i P_k u_{i,k}(1/2) = 1/2\ u_{i^*,k^*}(1/2)$$

$$= 1/4\ (d_{i^*,k^*} + d_{k^*,i^*})$$

$$\geq 1/4\ u_{i^*,k^*}(s^*) = E_2/4$$

For the completely asymmetric binary channel of Fig. 2-2, page 12, $E_2 = -\ln p$; $E_\infty = -1/4 \ln p$.

Upper bound solution: Let $\underline{P}^*$ maximize the expression for E_∞. Then select $\underline{x}$ and $\underline{x}'$ with $N_{i,k} = A P_i^* P_k^*$ for all $i \neq k$; $N_{i,i} = 0$ for all i. Then $N = \sum_i \sum_k N_{i,k} = A(1 - \sum_k P_k^{*2})$ $\geq A(K-1)/K$, because $0 \leq \sum_k (P_k^* - 1/K)^2 = \sum_k P_k^{*2} - 1/K$. By the construction

$$N\, E(\underline{x}, \underline{x}') = A\, E_\infty$$

$$E_2 \geq E(\underline{x}, \underline{x}') = A/N\, E_\infty \geq (K-1)/K\, E_\infty$$

Equality here holds for the K-level pairwise erasure channel which is uniform from the input. For such a channel each input a_k has an associated output b_k, which it reaches with $Pr(b_k/a_k) = q$, and each pair of inputs (a_i, a_k) have an associated output $b_{i,k}$ with $Pr(b_{i,k}/a_k) = Pr(b_{i,k}/a_k) = p$. No other transitions are possible so $q + (K-1)p = 1$. The total number of outputs is given by $J = \binom{K}{2} + K$, although for channels of this type the usual notation b_j, $j = 1, \ldots, J$ is cumbersome.

The K-level Hamming metric channel, with $J=K$, $p_{j,k} = q$ iff $j = k$, and $p_{j,k} = p$ iff $j \neq k$, (again $q + (K-1)\, p = 1$) also yields equality of the upper bound.

Exercise 2-2: Show that it is possible to do exponentially better than the repeated 8-word 1st order Reed-Muller code (1954) for the completely asymmetric binary channel.

Solution:

Reed-Muller		Improved	
0000000		000	
1111000		001	
1100110		010	
0011110		011	
1010101	Repeated N/7 times	100	Repeated N/3 times
0101101		101	
0110011		110	
1001011		111	
The exponent between the second and third words is -2/7 ln p.		The exponent between any two words is either -ln p or -1/3 ln p.	

Exercise 2-3: Nevertheless, show that the zero rate sequence of repeated 1st order Reed-Muller codes is asymptotically optimum for any binary input channel!

Solution: There are only two requirements for asymptotic optimality at the zero-rate point E_∞ : 1). Every column of the code must have the optimum composition, $\underline{P}^*$. 2) The code must be equidistant, with distances measured by the function $u_{i,k}(1/2) = u_{k,i}(1/2)$.

For any binary input channel, K = 2. There is only one distance,† as $\underline{P}^*$ = (1/2, 1/2). All group codes (including Reed-Muller) satisfy this composition requirement, and 1st order Reed-Muller codes are equidistant.

At positive rates, however, $\underline{P}^*$ may no longer be optimum. For example, the input distribution which attains channel capacity for the channel of Fig. 2-4, page 13, is different from (1/2, 1/2).

For multi-input pairwise reversible channels, there is no general expression for the optimum $\underline{P}$ even at zero rate. For example, for the channel of Fig. 2-5, page 13, $\underline{P}^*$ = (4/23, 9/23, 10/23).

† Distance here is $u_{i,k}(1/2)$, not $d_{i,k}$. See previous paragraph.

Exercise 2-4 For given small $M > 2$, find a necessary and sufficient set of conditions on the channel such that $E_M = E_2$.

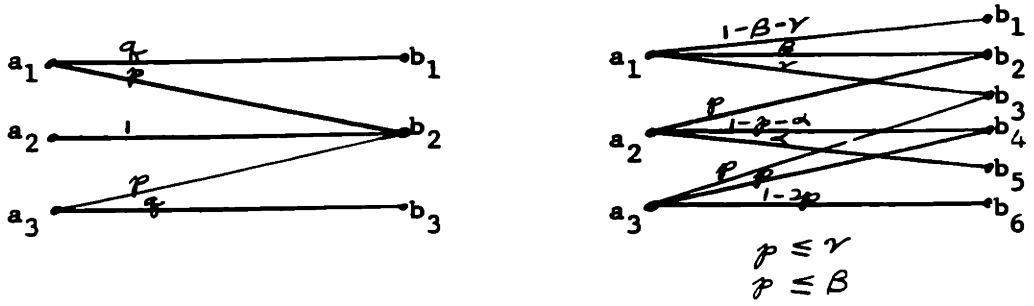
Solution: It is apparent that $E(\underline{x}_m, \underline{x}_{m'})$ must be the same maximum value for all input pairs $m, m' = 1, \ldots M$. This immediately requires that all M letters in any column of the code must be different. Thus $K \geq M$. Furthermore, there can be no harm in selecting each codeword entirely of the same input letter:

$$\underline{x}_m = a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k a_k \cdots$$

for some k(m). If all codes of this type fail, nothing else will work, for we have seen (pp. 15-16) that any mixing only reduces the exponent. If such a code works, then evidently the set S of M input letters satisfies the condition:

$$\max_s u_{i,k}(s) = u_{max} \quad \text{for all } i, k \text{ in } S$$

The existence of such a set S, containing M elements, is the necessary and sufficient condition. It may be guaranteed by certain symmetry properties of the channel, for example, pairwise uniformity $(u_{i,k}(s)) = u_{i',k'}(s)$ or $u_{k',i'}(s)$, for all pairs (i, k) and (i', k')). It may, however, be satisfied by channels without any such condition.



Asymmetric channels for which $E_3 = E_2 = -\ln p$.

Exercise 2-5 In view of the Very Noisy Channel result, one might conjecture that the following hold in general:

$$1)\quad 2R_{crit} \le R_{comp} \le 1/2\, C$$

$$2)\quad C \le E_{sp}(0)$$

$$3)\quad 2E_{\infty} \le E_{sp}(0)$$

Show by a single counterexample that all these conjectures are false.

Solution: (H. L. Yudkin and R. G. Gallager)

Consider the K-input erasure channel, with $J = K + 1$, defined by

$p_{K+1,k} = p_{k,k} = 1/2$ for all $k = 1, \ldots K$; $p_{j,k} = 0$ for $k \neq j \neq K+1$.

$$E_o(\rho) = \max_{\underline{P}} -\ln \sum_j \left(\sum_k P_k p_{j,k}^{\frac{1}{1+\rho}} \right)^{1+\rho} \qquad (1.10)$$

$$= -\ln \left(K \left(\frac{1}{K}\left(\frac{1}{2}\right)^{\frac{1}{1+\rho}}\right)^{1+\rho} + \frac{1}{2} \right) \quad (\text{Since } P_k^* = 1/K)$$

$$= \ln 2 - \ln (1 + K^{-\rho})$$

$$E_o'(\rho) = (\ln K)/(1 + K^{\rho})$$

As $K \to \infty$

$C = 1/2 \ln K \to \infty$

$R_{comp} = \ln 2 - \ln (1 + K^{-1}) \to \ln 2$

$R_{crit} = (\ln K)/(1 + K) \to 0$

$E_{sp}(0) = \ln 2 = \ln 2$

$E_{exp}(0) = ((K-1)/K) \ln 2 \to \ln 2$

ZERO-RATE EXPONENTS FOR CHANNELS WITH FEEDBACK

Chapter Abstract

In this chapter, we first consider an example for which the F(R) curve coincides with the Shannon-Gallager upper bound. This example provides an indication of the proof of that bound, and motivates our subsequent efforts to compute F_∞.

We find that, in general, $F_2 = E_2$. For larger M, however, F_M generally exceeds E_M. We succeed in computing F_∞ only for certain special classes of channels. In all known cases, $F_\infty = F_M$, for some finite M. In fact, we know of no example for which $F_\infty < F_3$. For channels whose best pair of inputs has only one common output, we prove that $F_\infty = F_2$. For channels which have every output inaccessible from at least I inputs (I>0), $F(0) = F_\infty = F_{K-I}$ (and possibly also $F_\infty = F_M$ for certain lesser M).

After considerable labor, we show that, for the binary symmetric channel, $F_\infty = F_3 < F_2$. The result generalizes to symmetric binary-input channels, giving

$$F_\infty = -\ln \sum_j p_{j,1}^{1/3} p_{j,2}^{2/3}$$

We show that these results remain valid if the noiseless feedback channel contains a small delay, so long as the delay is much shorter than the block length.

All of these results are obtained by examining the behavior of a certain constructive class of coding strategies, called order strategies. For any given M, we exhibit an asymmetric binary channel for which $F_M = F_2$, but $F_{M+1}^{(\text{order})} < F_2$, using any order strategy for M+1 codewords. It is not known whether nonorder strategies have this same limitation.

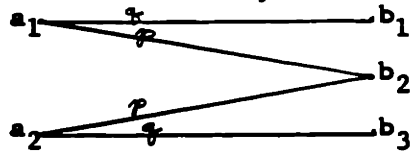
Chapter 3

ZERO RATE EXPONENTS FOR CHANNELS WITH FEEDBACK

Introduction

For some channels, coding with feedback presents no problems. The binary erasure channel, shown in Figure 3-1, is such a case.

Figure 3-1. The Binary Erasure Channel



One starts with an ensemble of $M = 2^{RN}$ codewords, or, equivalently, a message sequence containing RN bits. These bits are transmitted one by one across the channel. Whenever a bit is erased, it is repeated until it is received without erasure. A decoding error can occur only if the channel erases more than (1-R)N of the N transmitted bits. This happens with a probability that is asymptotically give by

$$P_e \approx \binom{N}{(1-R)N} p^{(1-R)N} q^{RN}$$

$$F(R) = H(1-R) - (1-R) \ln p - R \ln q$$

This curve F(R) coincides with the sphere-packing bound, $F(R) = E_{sp}(R)$, for all rates, $0 \leq R \leq C = q$. In particular, at zero rate we have

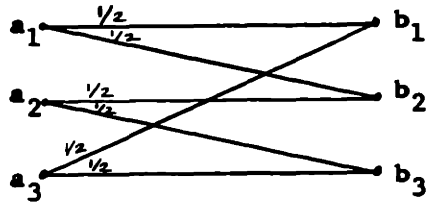
$$F(0) = E_{sp}(0) = E_2 = -\ln p$$

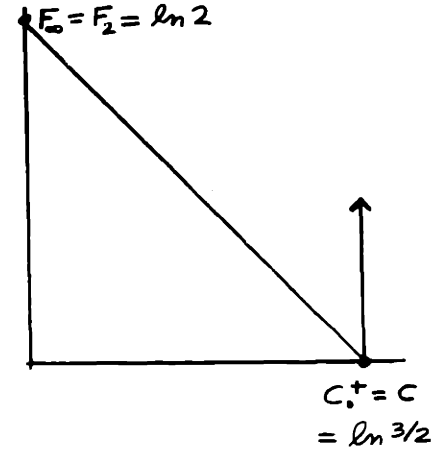
Furthermore, even with feedback, if the channel erases every bit, the probability of error is (1 - 1/M). Thus, $F_2 = F(0) = F_M$ for all M.

For most channels, the coding problem is considerably more complicated. Not only must our coding strategies be more sophisticated, but, in general, we will be unable to achieve the sphere packing exponent at low rates.

An example of what happens is given by the uniform, pairwise reversible ternary unilateral channel shown in Figure 3-2. This example was suggested by Prof. C. E. Shannon.

Figure 3-2.
Shannon's channel and its F(R) curve





For this channel, the sphere-packing bound degenerates into a wall located at $C = C_o^+ = \ln 3/2$. Yet, it is apparent that $C_o = 0$, for any two input symbols will lead to the same output symbol with probability 1/2. If two input sequences differ in every position, then they will be confused with an exponent given by

$$E_2 = \ln 2$$

Coding for this channel poses no great problem. From the receiver's viewpoint, at any stage, there is a certain set of input codewords which might be the selected message, and all of these possible messages are equally likely. The a posteriori probability of the other codewords is zero.

The best coding strategy trisects the possible messages at each transmission, placing 1/3 of them each on a_1, a_2, and a_3. Thus, if there are m_n possible messages after the first n questions, then after the first n+1 questions, there are $m_{n+1} = 2m_n/3$ possible messages. Taking into account the Diophontine constraints (i.e., m_n may not be divisible by 3), we can upper bound m_n by $\bar{m}_n$,

($\bar{m}_n$ is not necessairly an integer.) $\bar{m}_n$ satisfies

$$\bar{m}_{n+1} = 2/3\, \bar{m}_n + 1 \; ; \quad \bar{m}_0 = M$$

The solution to this recurrence is

$$\bar{m}_n = (2/3)^n (M-3) + 3$$

Hence, after asking $N_1 = \ln M / \ln (3/2)$ questions, we have

$$m_{N_1} \leq \bar{m}_{N_1} = (2/3)^{N_1} (M-3) + 3 = (M-3)/M + 3 < 4$$

Since m_{N_1} is integral,

$$m_{N_1} \leq 3, \quad \text{whence } m_{N_1+1} \leq 2$$

There still remain $N_2 = N-N_1$ or $N-N_1-1$ digits to be transmitted. The channel users can do no better than to play the two remaining possible words against each other at each of these final N_2 questions. Within a factor of 2, this gives

$$P_e = 2^{-N_2}$$

Thus

$$F(R) = N_2/N \ln 2 = (1- R/\ln 3/2) \ln 2$$

In particular, we again have

$$F(0) = F_\infty = F_2 = E_2$$

The general Shannon-Gallager (1965) upper bound on error exponents is obtained in a manner quite analagous to the procedure which is quite obvious for this simple special case. One argues that the probability of error is at least the product of the probability that the receiver finds L or more words at least as probable as the correct word after N_1 digits have been received, and the probability of error for (L+1) codewords with $N_2 = N-N_1$ digits. The first probability is bounded by the sphere packing bound; the second probability may be bounded by any known low-rate upper bound on exponents. When the overall bound is optimized over L and N_1, one finds that the resulting bound is tangent to

both the sphere packing bound and the low rate bound, as shown in Figure 1-3. For the channel of Figure 3-2, the best bound is attained with L=1 and $N_1 = \ln M / \ln 3/2$.

For channels such as the one shown in Figure 3-2(†) the Shannon-Gallager bound gives the correct F(R) curve, as we have seen. For most channels, unfortunately, there is no known coding scheme which achieves this bound. Nevertheless, this is the tightest bound known. For this reason, we shall devote the remainder of this chapter to calculation of the zero-rate exponents, with the intention of using the point F_∞ as an origin for the Shannon-Gallager bound. We must confess that our methods do not yield lower bounds at positive rates, and we are not even able to prove that our answers are correct at rate ϵ, for conceivably $F(0) < F_\infty$. There is a good deal of heuristic evidence, some of which will be considered in Chapter 4, against such conceptual possibilities. We are led to conjecture that, for channels with feedback, the Shannon-Gallager upper bound on exponents, drawn from F_∞ to the sphere packing bound, can always be achieved. We have seen that this is true for certain special channels. In chapter 4 we shall exhibit constructive procedures which come very close to achieving this bound for the binary symmetric channel.

For the remainder of this chapter, we direct our efforts toward the computation of F_∞.

(†) Generalizations of this case are considered in Exercises 3-4 and 3-6.

For the simplest case, (M = 2), F_M is known. Shannon and Gallager have shown that, in general, $F_2 = E_2$. The proof of this theorem is similar to the proof that $F(R) \leq E_{sp}(R)$.

Note that this result does <u>not</u> say that the probability of error for two codewords is not improved with the use of feedback. In some cases it is (c.f. Exercise 3-3). The theorem guarantees that any such improvement is not exponential in N.

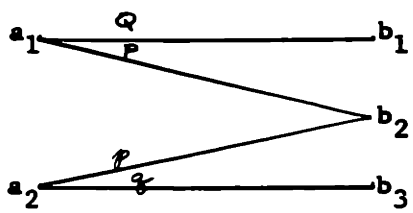
We have seen that for the channels of Figures 3-1 and 3-2, $F_\infty = F_2$. Exercise 3-7 contains one straightforward generalization of that result. The following theorem gives another generalization.

<u>Theorem</u>:
If the best pair of inputs reach only one common output with nonzero probability, then $F_\infty = E_2$.

The best pair of inputs is that i,k which maximizes the expression for $F_2 = E_2$ (Equation (2.08), p. 15)

<u>Proof</u>: Since we shall use only the best pair of inputs, we may restrict our considerations to them. Without loss of generality, we then have the asymetric binary erasure channel of Figure 3-3.

Figure 3-3 The asymmetric binary erasure channel



$P + Q = 1 = p + q$

$p \leq P$

$\max_{0 \leq s \leq 1} u_{1,2}(s) = -\ln p$

Our coding strategy is very simple. We place one codeword on a_1 and the remaining M-1 codewords on a_2. As long as we receive the output b_2, we continue transmitting the same thing. If we ever receive an output b_1, we know that the lone word currently at a_1 is the selected message, and we may quit. If we ever receive an output b_2, we know that the lone word at a_1 is not the message, so we discard it from further consideration and move one of the words at a_2 up to a_1 to replace the discarded word. If we reach the end of the block without ever receiving a b_1, the decoder selects the lone word at a_1 as his choice of the selected message.

An error can occur only if the correct message remains at a_2 throughout the block. The total number of discarded words cannot exceed M-2. Thus, the probability of error is bounded by

$$P_e \leq \sum_{m=0}^{M-2} \binom{N}{m} p^{N-m} q^m$$

$$F_M = \lim_{N\to\infty} -1/N \ln P_e = -\ln p = F_2$$

Since this holds for all M, it also holds for F_∞

q.e.d.

Other investigations have revealed other classes of channels for which $F_\infty = F_2$. Notable among these cases are the K-level Hamming-metric channels, $K > 2$. Such channels have K inputs and K outputs, with each input leading to its corresponding output with a probability q, and to each wrong output with probability p. $q + (K-1)p = 1$. This channel is the multi-level generalization of the binary symmetric channel for which the one-way codes of Peterson (1961) et. al. are designed. Unfortunately our argument that $F_\infty = F_2$ is lengthy and tedious. Parts of the proof have not yet been completely rigorified, and for this reason we will not present the proof here. There are indications that this result can also be extended to all K-level channels (K>2) which are uniform from the input, although this statement must presently be treated as an open conjecture.

CODING FOR THE BINARY SYMMETRIC CHANNEL

Introduction

We now consider the problem of coding for the binary symmetric channel (Figure 2-1) with noiseless, delayless feedback. In this chapter we shall evaluate F_{∞}; in Chapter 4 we shall consider strategies at positive rates. We will often refer to the coding process as a game between two hostile opponents: Coder, a partnership including the transmitter and the receiver, and Nature, who controls the channel transitions.

The game of transmitting one block of information on this channel is played as follows: Originally the source selects one message from an ensemble of M words. He attempts to convey this choice to the receiver by transmitting N bits across the noisy channel. Some of these transmissions may depend on information the source receives from the feedback channel as well as on the selected message word.

We adopt the point of view that just prior to each forward transmission the receiver asks the source a yes-no question: "Is the correct message among the set S_i?" (S_i is a subset of the M possible messages.) The question is transmitted back to the source over the noiseless feedback link, and the source's answer is then sent to the receiver via the noisy channel. The source receives a noisy answer, and then asks another question. At each stage the questioned set, S_i, may depend on the entire past history of the game.

It may first appear that this viewpoint necessitates an unusually large amount of feedback, since at each stage the receiver transmits back a subset S_i, which may be any subset of M possible message words. This transmission seems to require $\log_2 M$ bits of noiseless feedback. Actually, however, only one bit of feedback is required for each bit transmitted, because the transmitter may be endowed with the same deterministic subset-selecting machine as the receiver. The only inputs into this

subset-selector are the results of previous questions, i.e. the received sequence of bits. Thus the evolution of the questioning process is determined only by the received sequence of answers. If the feedback channel can accommodate one noiseless bit for each noisy bit sent down the forward channel, the source can be kept informed of the received sequence. He then knows as much as the receiver, and additional feedback cannot be of any additional help.

Any strategy may be viewed as a clean-question, noisy-answer process of the type just described. One need only consider the set of possible selected messages which would cause the source to transmit a one next, and call this the questioned set. The question-answer viewpoint involves no restriction on the types of strategies permissible.

The receiver may regard each answer he receives as a vote against a certain subset of words. As the process proceeds, different words acquire different numbers of unfavorable votes. After all N transmitted bits are received, the receiver must decide which word was transmitted. He obviously does best to select that word which has received the fewest unfavorable votes.

As an example, let us suppose that M = 8, N = 11. We denote the 8 possible messages by A,B,C,D,E,F,G,and H. We start with all 8 codewords having no votes against them, and 11 questions remaining. The game might proceed as shown in Figure 3-4a.

Votes Against	Questions Remaining: 11	10	9	8	7	6	5	4	3	2	1	0
0	ABCDEFG	ADEH	DE	D	D							
1		BCFG	ACFH	CEF	F	DF	F					
2			BG	AGH	ACE	A	AD	ADF	DF	F		
3				B	BGH	BCEG	EG	-	A	AD	ADF	A
4						H	BC	BCEG	EG	-	-	DF
5							H	-	BC	BCEG	EG	-
6								H	-	-	BC	EGBC
7									H	-	-	-
8										H	-	-
9											H	H

Figure 3-4a A Sample Game

For example, when there were 5 questions remaining, the receiver asked the question: "Is the selected message among the set FEGH ?" The reply that was received was "No".

In this game, Nature caused at least three channel errors. If it caused only three errors, than A was the selected message, and Nature's errors occurred at questions 10, 9, and 4. It is also possible that D was the selected message, in which case Nature caused four errors, at questions 7,6,3, and 1; or that F is the message, in which case the four errors occurred at questions 11,5,2, and 1. If any of the other codewords was the message, then Nature committed six or more errors.

In Chapter 4 we shall consider the number of words at each level as a function of the number of questions remaining. For the game just shown, this function is

Votes Against	Questions Remaining: 11	10	9	8	7	6	5	4	3	2	1	0
0	8	4	2	1	1	0	0	0	0	0	0	0
1		4	4	3	1	2	1	0	0	0	0	0
2			2	3	3	1	2	3	2	1	0	0
3				1	3	4	2	0	1	2	3	1
4						1	2	4	2	0	0	2
5							1	0	2	4	2	0
6								1	0	0	2	4
7									1	0	0	0

Figure 3-4b
Numbers of words at various levels

In this chapter, we will sometimes refer to the trajectory of a given word. For example, we may use Roman numeral subscripts, W_I and W_{II} to denote the words which finished first and second. x_I and x_{II} (both functions of n, the number of questions remaining) denote the number of votes against these words, respectively. The trajectories of x_I and x_{II} for the game of Figure 3-4a are shown in Figures 3-4c and 3-4d

Votes against	Questions remaining											
	11	10	9	8	7	6	5	4	3	2	1	0
0	x_I	x_I										
1			x_I									
2				x_I	x_I	x_I	x_I	x_I				
3									x_I	x_I	x_I	x_I
...												

Figure 3-4c
The Trajectory of W_I (codeword A)

Votes against	Questions remaining											
	11	10	9	8	7	6	5	4	3	2	1	0
0	x_{II}	x_{II}	x_{II}	x_{II}	x_{II}							
1						x_{II}						
2							x_{II}	x_{II}	x_{II}			
3										x_{II}	x_{II}	
4												x_{II}
5												

Figure 3-4d
The Trajectory of W_{II} (codeword D)

Some of our proofs in subsequent sections of this chapter require arguments based on the trajectories of the currently most probable word, or the currently second most probable word,... We denote the most probable word by W_1, and the number of votes against it by x_1; the currently second most probable word by W_2 and the number of votes against it by x_2,... The reader is warned not to be confused by our use of x_1 as the number of votes currently <u>against</u> the most probable word. Thus, $x_1 \leq x_2 \leq x_3 \leq \cdots$

even though we talk of W_I as being on top of the list. Although perhaps this terminology gives rise to unnecessary confusion in the remaining portions of this chapter, any other definitions would be inconsistent with the investigations we pursue in Chapter 4, and the natural point of view adopted there.

Figure 3-4e plots x_1, the trajectory of W_1, for the game of Figure 3-4a.

Votes Against	Questions remaining: 11	10	9	8	7	6	5	4	3	2	1	0
0	x_1	x_1	x_1	x_1	x_1							
1						x_1	x_1					
2								x_1	x_1	x_1		
3											x_1	x_1
4												
...												

Figure 3-4e The trajectory of the currently most probable word

Order strategies

Among the various strategies available to Coder, some strategies have the property that the words are partitioned into the two questioned subsets in a manner which depends only on the order of their probabilities, as viewed by the receiver. For example, in the game of Figure 3-4a, Coder used an order strategy which always played the first, fourth, fifth, and eighth words against the second, third, sixth, and seventh. He broke ties by conventionally using alphabetical order among words which had equal numbers of votes against them.

Notice that sometimes in the course of the game, word that was W_j becomes W_{j+1} and vice versa. Such an occurrence is called a j,j+1 crossunder. In the game of Figure 3-4a, 1,2 crossunders occurred at questions 10, 6, 5, 4, 3, and 2.

Because of crossunders, it is difficult to count the number of ways in which the words can end up in various positions. However, averages which include all the words whose labels change at the

crossunder can be more readily enumerated. Since we shall have frequent use for these averages, we introduce a special notation:

Definition: $$x_{j,k} = 1/(k-j+1) \sum_{i=j}^{k} x_i$$

For example, $x_{1,3}$ is the average of the top three words. A plot of this average for the game of Figure 3-4a is given in Figure 3-4f.

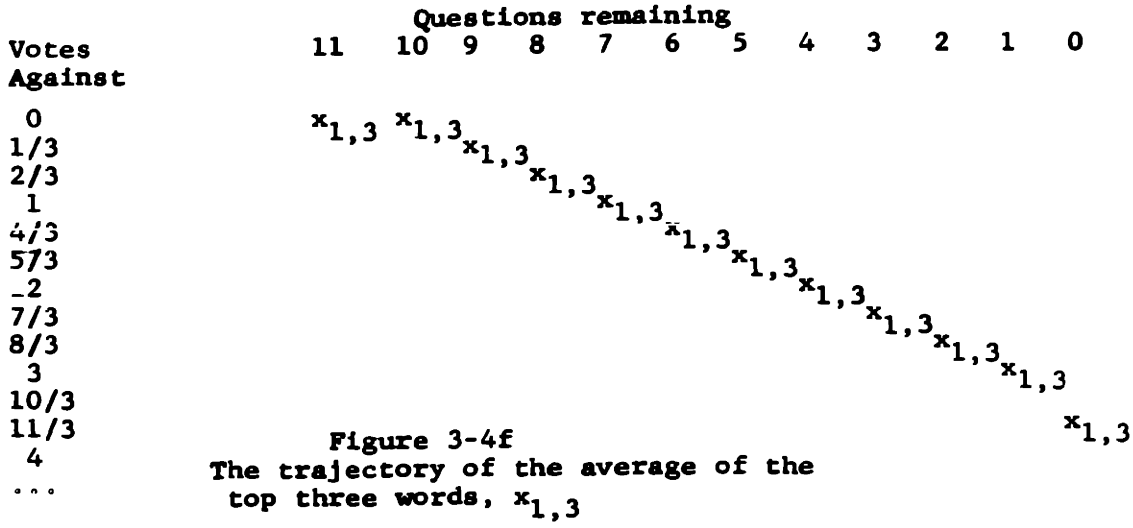


Figure 3-4f
The trajectory of the average of the top three words, $x_{1,3}$

Most of the remainder of this chapter is devoted to a detailed study of the behavior of certain order strategies for the binary symmetric channel at zero rate. We first compute F_3, then F_5, and finally, F_M.

In order to minimize the number of crossunders, it is convenient to relabel the words as infrequently as possible, rather than to adopt a fixed (alphabetical) ordering for breaking ties. Thus, if A and B both have the same number of negative votes, we call W_1 whichever of them was most recently ahead. Only if they have been tied throughout all previous questions do we use the alphabetical ordering to label tied words.

3 CODEWORDS

Any reasonable strategy for partitioning three codewords has the property that it always asks one of the words against the other two. If the single word falls, $x_{1,3}$ falls by 1/3; if the pair of words falls, $x_{1,3}$ falls by 2/3. If, after N questions have been asked, the pair of words have kallen k times, then the lone word has fallen N-k times and the average has fallen (N+k)/3. There are $\binom{N}{k}$ different sets of k questions at which the two words can fall; thus there are precisely $\binom{N}{k}$ ways in which the average of the three words can end up at $x_{1,3} = (N+k)/3$. This is true for any strategy which does not waste any questions by asking all three words against nothing.

The strategy which always plays the most probable word against the other two has an additional property which enables us to bound its error probability: there is never more than one word much above average. To show this we first observe that the second and third words are always within one vote of each other. $x_2 \leq x_3 \leq x_2+1$. This observation is readily proved by induction. Initially $x_2=x_3$. By considering the possible cases which can cause one of these words to change labels with x_1, we find that there is no way to separate the bottom two words. Each question partitions them into the same subset. From

$$x_1 \leq x_2 \leq x_3 \leq x_2+1$$

we conclude that

$$x_2 \geq x_{1,3} - 1/3, \quad \text{with equality iff } x_1 = x_2 = x_3-1.$$

The probability of any given particular pattern of e channel errors which causes some wrong word to end up on top is given by $p^e q^{N-e}$. The right word ends up with e votes against it, so either $x_2=e$, or $x_3=e$. In either case $e \geq x_{1,3} - 1/3$, so

$$p^e q^{N-e} \leq (q/p)^{1/3} \, p^{x_{1,3}} \, q^{N-x_{1,3}}$$

This bounds the probability of error for any particular path by which the average ends up at $x_{1,3} = (N+k)/3$. We have observed

that there are $\binom{N}{k}$ such paths. Thus, the probability of error is bounded.

$$P_e \leq \frac{\sum_i \binom{N}{i} p^{(N+i)/3} q^{(2N-i)/3}}{p^{1/3} q^{-1/3}} = \frac{(p^{1/3}q^{2/3} + p^{2/3}q^{1/3})^N}{p^{1/3}q^{-1/3}}$$

After investigating certain properties of this bound, we shall be able to show that it is exponentially optimum. No strategy for three codewords can do exponentially better.

Asymptotic Properties of the Bound

The Dominant Term

If a sum of positive terms $\sum_{k=0}^{N} a_k(N)$ approaches zero exponentially in N, then for large N the sum is exponentially dominated by the maximum term. This maximum term is often most readily found by setting the ratio $a_{k+1}/a_k = 1$ and solving for k as a function of N, assuming N large.

In the above case this gives

$$a_k = \binom{N}{k} p^{(N+k)/3} q^{(2N-k)/3} \; ; \quad a_{k+1}/a_k = (N-k)\, p^{1/3}\, q^{-1/3}/k$$

This ratio =1 iff $k = k_{max} = N/(1+(q/p)^{1/3})$

As p varies from 0 to 1/2, k_{max} varies from 0 to N/2.

In order to show that $(p^{1/3}q^{2/3} + p^{2/3}q^{1/3})^N$ is an exponentially optimum bound, it is sufficient to show that the number of paths ending with the first and second words tied at $(N+k_{max})/3$ has the same exponential behavior as $\binom{N}{k_{max}} = 2^{NH(k_{max}/N)}$.

Ignorable Terms(†)

The total number of paths which take the right word down to a level e is given by $\binom{N}{e}$. If $\binom{N}{e} p^e q^{N-e} \leq (p^{1/3}q^{2/3} + p^{2/3}q^{1/3})^N$ there is no error in exponent if we assume that all paths of e errors will be incorrectly decoded. A particular value of e satisfies the above inequality iff $e \geq e_{ig}$, where e_{ig} is a fraction of N which may be determined by equating the two sides of the above inequality and solving. The solution is messy and unenlightening. It suffices for our purposes to note only that

$$(N+k_{max})/3 < e_{ig} < N/2 \text{ for any } 0 < p < 1/2$$

In particular, there is never any exponential error in assuming that all patterns of N/2 or more errors will cause a decoding failure. We shall use this fact frequently in our calculations of the exponents for 5 codewords, and for M codewords.

A Lower Bound to the Probability of Error with Three Codewords

In order to derive a lower bound to the probability of error, we will show that for any coding strategy, and any $k < N/2$, there are an exponentially large number of paths ($2^{NH(k/N)}$) which end with $x_1 \leq x_2 \leq (N+k)/3$. Since in particular this result holds for k_{max}, it will follow that for any coding strategy, the probability of error is exponentially no better than that for the strategy which always plays the top word against the other two.

At the beginning of the game, Coder must let Nature know N and p (and hence $k_{max} = K$). However, he need not give her any hints concerning what strategy he plans to use. He may change this strategy in the course of the game depending on how Nature happens to be plotting against him.

(†) The result of this subsection is not used in the following section, but it is given here for future reference.

The strategy by which Nature clobbers Coder is the following: Two words must be kept above (N+K)/3 in essentially $\binom{N}{K}$ ways. Define $y_i = (N+K)/3 - x_i$. Then $y_1 \geq y_2 \geq y_3$. As the game procedes, the y's decrease. Eventually y_3 may go negative, Nature plans to keep y_2 and y_1 positive. Initially, $y_{1,3} = (N+K)/3$. During the first part of the game, Nature need only track this average and keep it sufficiently large. Specifically, let Nature play so that for any r, when there are r questions remaining, $y_{1,3} \geq r(K+N)/3N$. We show in Appendix A that the number of ways of accomplishing this fete for all r = N, N-1,...R is exponentially equivalent to the number of ways of accomplishing it only for r=R. This is the number of ways of selecting the (N-r)K/N times that a pair of words falls from the (N-r) questions, or $\binom{(N-r)}{(N-r)K/N}$. Now as long as all three words remain sufficiently close to their average, Nature can continue tracking only the average. If, however, the second and third words fall sufficiently far below average, disaster threatens. Both y_2 and y_3 may fall negative, although the average remains quite high because y_1 is large. When this situation is imminent, Nature must abandon the third word entirely, and track the second one. By concentrating on keeping this second one up, Nature can ensure that both y_1 and y_2 remain positive.

The time when Nature abandons the average is determined by the condition $y_3 \leq rK/N \leq y_2 < rK/N + 1$. When this happens, $y_{1,3} \geq r(N+K)/3N$, and hence $y_1 = 3y_{1,3} - y_2 - y_3 \geq r(N-K)/N - 1$

Let W_{II} be the word then at y_2, and W_I the word at y_1. These two words may subsequently change places, but we will <u>not</u> change their labels. For the final r questions, Nature takes care to vote against W_{II} no more than rK/N times, and against W_I no more than r - rK/N times. If these two words are pitted against each other at every question (Coder's best attempt), then Nature can do this in $\binom{r}{rK/N}$ different ways. If Coder wastes some questions

by playing these two words together, Nature must avoid voting against both of them the first time such a question is asked, but on successive wasted questions Nature has more options. She can get in j votes against them both out of the first w wasted questions in $\binom{w}{j}$ different ways. By the theorem of Appendix A, this can be done so that the first W wasted questions always have no more than J = Wj/w negative votes, with no exponential loss in the number of such combinations. Thus Nature can keep y_1 and y_2 positive for the last r questions in essentially $2^{rH(K/N)}$ different ways.

We conclude that the number of paths by which Nature can keep $x_1 \leq x_2 \leq (N+K)/3$ is exponentially $2^{(N-r)H(K/N)}\ 2^{rH(K/N)} = 2^{NH(K/N)}$. r is the number of questions after which Nature switches from tracking the average to tracking only the top two words. Coder has some control on r, but it does him no good. For any r that he might wish to select, Nature still retains the ability to hit him with the maximum exponent. Thus, for any feedback strategy for transmitting three codewords,

$$F_3 \leq -\ln (p^{1/3}q^{2/3} + p^{2/3}q^{1/3})$$

Middle word vs the Top and Bottom

Introduction

We next consider another strategy for playing three codewords: always ask the middle word against the top and the bottom.

This analysis will show that the abrupt change in Nature's strategy which was described in the previous section is no mere figment of our bounding procedure. Against the coding strategy which plays the middle word against the top and bottom words, the dominant terms in the probability of error are those which arise from such nonuniform behavior by Nature.

The techniques of analysis introduced in this section are quite similar to those which we use in subsequent sections. They are introduced here in a simple setting where they can be

more readily understood.

Our major goal is to show that this strategy is exponentially as good as the strategy which always plays the top word against the bottom two. In order to do this, we will show that for any $k < N/2$, there are exponentially no more than $\binom{N}{k}$ paths in which the second word ends up above $(N+k)/3$.

The number of paths which leave two words above $(N+k)/3$

Throughout this subsection, we assume that N and k are fixed. All paths we consider have the property that they end with $x_2 \leq (N+k)/3$. We first classify all such paths according to the question at which the second and third words last exchanged places. Let N_b be the number of questions before this final crossunder occurred; let N_a be the number of questions after (and including) this final crossunder. At the final crossunder between x_2 and x_3, let W_I, W_{II} and W_{III} denote the words emerging at x_1, x_2, and x_3. These labels are kept on these words for the rest of the game, even though W_I and W_{II} may subsequently crossunder each other.

We now define the quantities k_a and k_b in a deliberately inconsistent manner.

Let k_a be the number of times W_{II} fell during the last N_a questions.

Let k_b be the number of times the first and third words fell during the first N_b questions.

The number of times the second word fell during the first N_b questions is given by $N_b - k_b$, and the average of the top three words after the first N_b questions is $(N_b + k_b)/3$. At this point, however, $x_2 = x_3 \leq (N+k)/3 - k_a$. (Recall that W_{II}, which falls exactly k_a times in the final N_a questions, is one of the two words which ends above $(N+k)/3$.) Thus, at the final crossunder,

$$x_1 = 3x_{1,3} - x_2 - x_3 \geq N_b - k_b - 2(N+k)/3 + 2k_a$$

During the last N_a questions W_I and W_{II} were always the first and second words (in one order or the other), and were always asked against each other. Hence, W_I fell $N_a - k_a$ in the last N_a questions. Since W_I was one of the two words which ended above $(N+k)/3$, we conclude that at the crossunder point,

$$x_1 \leq (N+k)/3 - (N_a - k_a)$$

Comparing this with the previous formula gives

$$N_b + k_b - 2(N+k)/3 + 2k_a \leq (N+k)/3 - N_a + k_a$$

which reduces to

$$k_a + k_b \leq k$$

We define the sum of k_a and k_b as $k_s = k_a + k_b$

The number of paths with given N_a, N_b, k_a, k_b is overbounded by $\binom{N_a}{k_a}\binom{N_b}{k_b}$ The number is actually less than this, for some subsets of k_b of the first N_b questions do not end with $x_2 = x_3$, and some subsets of k_a of the final N_a questions cause x_2 to cross under x_3 again. Nevertheless, this expression is a valid (but weak) upper bound. The total number of paths is bounded by summing over all possible values of N_a, N_b, k_a, and k_b

$$\text{Number of paths} \leq \sum_{N_a+N_b=N} \sum_{k_a+k_b=k_s} \binom{N_a}{k_a}\binom{N_b}{k_b} = \sum_{N_a+N_b=N} \binom{N}{k_s} = N\binom{N}{k_s}$$

Since $k \geq k_s$, $p^{(N+k)3}\, q^{(2N-k)/3} \leq p^{(N+k_s)/3}\, q^{(2N-k_s)/3}$

Hence,

$$P_e \leq \sum_{k_s} N \binom{N}{k_s} p^{(N+k_s)/3}\, q^{(2N-k_s)/3} = N(p^{1/3}q^{2/3} + p^{2/3}q^{1/3})^N$$

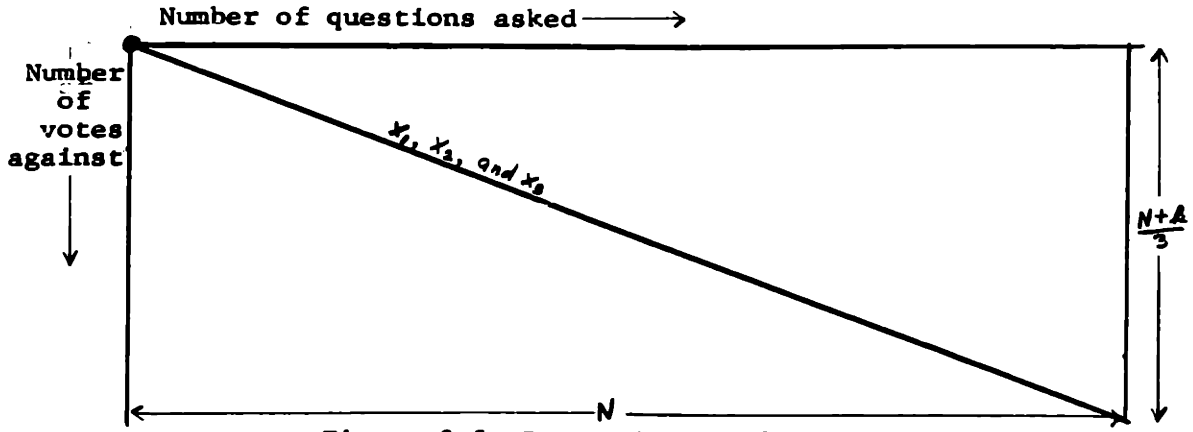
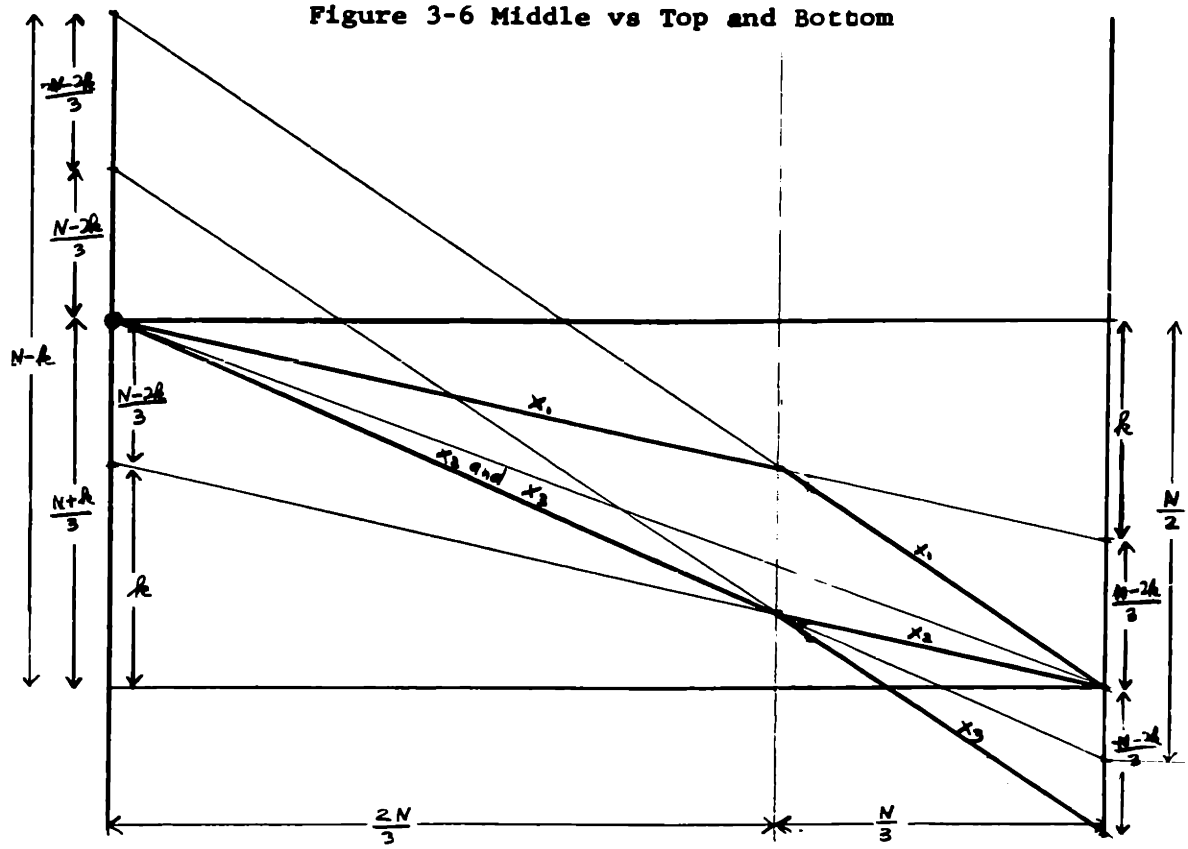


Figure 3-5 Top vs Bottom 2

$$k = k_{max} = N/[1+(q/p)^{1/3}]$$

Figure 3-6 Middle vs Top and Bottom



In the double sum for the number of paths, the dominant term is the one for which $k_a/N_a = k_b/N_b = k/N$. To do the most harm, before the final crossunder between the second and third words, Nature must let the first and third words drop with a frequency $k_{max}/N < 1/2$, but after the final crossunder, Nature should let the second word drop with this frequency. Figure 3-6 shows a smoothed out plot of this dominant error pattern. All the dimensions are given on the graph. A straightforward calculation of the intersection of the initial $x_2 = x_3$ line with the line at which Nature changes strategies reveals that this event occurs just after 2/3 of the questions have been asked. This transition point of the dominant error pattern is independent of k_{max} and p.

Conclusions About 3 Codewords

We have seen that for three codewords, an optimum probability of error may be attained by either of two order strategies. The bound on the probability of error for the strategy which asks the middle word against the other two is a factor of N worse than the bound on the probability of error for the strategy which always asks the top word against the bottom two. However, this extra factor is felt to be caused by the bounding procedure rather than by the strategy.

The dominant error patterns are those in which the average descends too slowly until some critical time at which the second and third word are sufficiently low. For the remainder of the block, the third word sinks to the depths, but the second word descends too slowly. Finally, both the second word and the first word end up with approximately $(N+k_{max})/3$ votes against each of them.

The critical point at which Nature switches strategies depends heavily on the coding strategy employed by the channel users. If Coder always plays the top word against the other two, most error patterns occur when the top word never gets much above the others.

In fact, using random walk theory(†) it can be shown that if there is an error, with overwhelming probability no word was ever more than about $N^{1/2}$ votes above the other two. Because of this, the second and third words will probably not fall below Natures's crossover line until almost the end of the block. The switch in Nature's strategy might well go unnoticed. (c.f. Figure 3-5)

If instead Coder always plays the middle word against the other two, Nature is forced to let one word temporarily remain a considerable distance above the others. This is the only way that Nature can keep the average up during the first two-thirds of the block. During the last third of the block, however, Nature abandons one of the bottom two words and causes the top word to sink back to the level of the second one. At the end of the block, the decoder is unable to decide between the word which got off to the big initial lead and the word which just barely caught up with it by a gallant finish.

Since both of the coding strategies we have examined are exponentially optimum, it appears that any hybrid strategy, which always plays the two top words against each other but assigns the bottom word arbitrarily, is also exponentially optimum. Conceivably one could also attain optimum exponential behavior by including some questions which play the bottom word against the top two,

(†) One can, in fact, obtain an explicit generating function for the probability of error with three codewords using the order strategy which always plays the top word against the bottom two. Starting from the random walk formula given by Feller (1950,p.319), one can obtain a generating function for the last crossunder. The denominator of this generating function (letting s be the variable of enumeration) is $8p^2qs^3 - ((1-4pqs^2)^{1/2})^3$. By examining the poles of this generating function in the complex plane, one can deduce the same asymptotic results we have presented here.

so long as all such seemingly poor questions occur at the very first part of the block. Near the end of the block such questions are virtually wasted. Without feedback there is a certain nonneglible fraction of the questions at the end of the block which must be of this type. That is precisely the reason why it is possible to do better with feedback. F_3 is greater than E_3.

The Invariance of Exponent to Small Delay

We show here that the probability of error is exponentially unchanged if a small delay of T bits is inserted into the noiseless feedback channel.

Let Coder adopt the strategy which plays the top word against the other two. Because of the feedback delay, the transmitter will not know which word is currently on top, but he does know which word was on top T bits ago. This is the word he asks against the other two. For all the first T questions, before any feedback is received, he plays one arbitrarily selected word against the other two.

Using this strategy, Coder prevents the difference in votes between the second word and the third word from exceding T,

$$x_{1,3} - x_2 \leq 2T/3$$

$$P_e \leq (q/p)^{2T/3} \left(p^{1/3}q^{2/3} + q^{2/3}p^{1/3}\right)^N$$

The probability of error is exponentially unchanged if $T \ll N$.

Similar arguments can be used to show that other feedback exponents we derive in this chapter are uneffected by sufficiently small delays.

5 CODEWORDS

Introduction

We now consider a particular order strategy for 5 codewords:

W_1

W_2
W_3

W_4
W_5

The second and third words are always asked against the other three. There are several obvious restrictions on the types of situations which can arise when this strategy is used. We first note that the second and third words remain together, and the fourth and fifth words remain together.

$$x_2 \leq x_3 \leq x_2 + 1 \qquad x_4 \leq x_5 \leq x_4 + 1$$

This restriction is very similar to that which arose for three codewords when the top one was always played against the bottom two. The proof again is a straightforward induction argument which is established by verifying the claim in the various possible crossunder situations. The other property of this strategy is that the difference between the positions of the top and bottom words, $x_5 - x_1$, cannot decrease.

There are now two basically different types of crossunders possible. One occurs when the right side of the partition (W_2 and W_3) drops; the other occurs when the left side (W_1, W_4, W_5) drops. The former is called a right crossunder; the latter, a left crossunder. Immediately preceding a left crossunder, $x_1 = x_2$ After this crossunder occurs, the labels on W_1 and W_2

(or possibly W_1 and W_3) must be interchanged. After the interchange of labels, x_1 is the same as it was before. However, x_5 increased because W_5 sunk with the left side of the partition. Thus any left crossunder increases the difference between the top and bottom words, $x_5 - x_1$.

Right crossunders occur when $x_3 = x_4$ and the right side then drops. Following a right crossunder, the labels on W_3 and W_4 (and possibly W_2 and/or W_5) must be interchanged. The difference $x_5 - x_1$ may or may not be increased by a right crossunder. The difference $x_{4,5} - x_1$, however, is always increased by any right crossunder.

The details of the four possible right crossunders are given in Figure 3-7.

Figure 3-7 Crossunder Details

Before	After
$x_4x_5 \quad x_2x_3$	$x_4x_5 \quad x_2x_3$
$x_4x_5 \quad \begin{matrix} x_2 \\ x_3 \end{matrix}$	$\begin{matrix} x_4 \\ x_5 \end{matrix} \quad x_2x_3$
$\begin{matrix} x_4 \\ x_5 \end{matrix} \quad x_2x_3$	$x_4x_5 \quad \begin{matrix} x_2 \\ x_3 \end{matrix}$
$\begin{matrix} x_4 \\ x_5 \end{matrix} \quad \begin{matrix} x_2 \\ x_3 \end{matrix}$	$x_4x_5 \quad x_2x_3$

Notice that immediately following the crossunder, we always have $x_5 = x_2 + 1$.

The average $x_{1,5}$ increases by 3/5 iff the right side of the partition drops, and by 2/5 iff the left side drops. This average is always well-behaved, even when crossunders occur. Other averages are not so polite. Except on right crossunders, $x_{1,3}$ increases by

1/3 iff the left side drops, and by 2/3 iff the right side drops. On right crossunders, however, $x_{1,3}$ may increase by 1/3, or it may not increase at all, even though the right side drops. Similarly, x_1 increases iff the left side drops, except on left crossunders. In conclusion, $x_{1,3}$ is well-behaved except at right crossunders; x_1 is well-behaved except at left crossunders.

Outline of proof that this order strategy is exponentially optimum

Our plot to bound the error probability for this strategy is essentially this: we will divide the N questions up into various regions, such that in each region some of the averages are well-behaved (although others need not be). Within any given region, we will track the well-behaved averages, and then relate them to each other at the boundaries between the regions. At the end of the game, we are interested in the average of the top three words, $x_{1,3}$. We will show that the number of paths by which this average can end up at (N+H)/3 is exponentially no more than $\binom{N}{H}$, for any $0 < H < N/2$. Since all words but W_1 are essentially below this average ($x_2 \leq x_{1,3} - 1/3$), the probability of error for any such path is bounded by the probability of the right word ending below $x_{1,3}$. The result then follows just as it did for three codewords when the top one was consistently played against the second and third.

The details are given in five parts.

Part 1) Partitioning the block into well-behaved regions
Part 2) Definitions of H_i and L_i
Part 3) Behavior of averages
Part 4) Bounding the number of regions
Part 5) Bounding the number of paths

Part 1) Partitioning the block into well-behaved regions

Definition: A region is a set of consecutive questions.

We now divide up the block into four types of regions according to the following plan. All consecutive crossunders of the same type are placed in the same region. These regions are called right regions or left regions, respectively, depending on whether they contain right crossunders or left crossunders. A right region starts with a right crossunder and ends with a right crossunder; a left region starts with a left crossunder and ends with a left crossunder. Left regions contain no right crossunders, and vice versa.

The questions in between left regions and right regions contain no crossunders at all. These questions comprise a transition region. A transition region begins just after a crossunder of one type, and ends just before a crossunder of the other type. Transition regions are called left-right regions or right-left regions, depending on whether they are preceded by a left region and followed by a right region or vice versa.

Non-transition regions must contain at least one crossunder. As a minimum, such regions contain only one question. Transition regions, on the other hand, have no such restrictions. Suppose, for example, that W_1,W_4, and W_5 fall on the first question. After relabeling, W_2 and W_3 fall next. The first question is a left region; the second question begins a right region. The left-right transition region between them is empty.

As stated above, our procedure ambiguously defines the region following the last crossunder. The ambiguity is resolved by the assumption that a left crossunder would occur before any right crossunders if the game were continued. Thus, if the final crossunder is a left crossunder, all subsequent questions are considered part of that left region; if the final crossunder is a right crossunder, the subsequent questions are considered as a right-left region.

Since this assumption is taken as a part of the rules for partitioning the block into regions, it logically requires no further justification. Nevertheless, we note that it makes good sense. If a decoding error occurs, it is very likely that the top two words end very close to each other, the correct one finishing second. If the questioning process were continued, another 1,2 crossunder might be expected very soon.

Part 2) Definitions of H_i and L_i

In the proof of the exponential optimality of the 3 codeword strategy which always played the middle word against the other two, we defined numbers k_i differently in different regions. In a similar manner, we now define numbers H_i and L_i.

In any given region H_i and L_i are the number of right falls and left falls, in one order or the other depending on the type of region. We use the notation H_i for the heavy side and L_i for the light side. In a right region or a left-right region we are interested in the top five words, and the left side is heavier; in a left region or a right-left region, we are interested in the top three words, and the side is heavier. In either case

$$H_i + L_i = n_i$$

One of the reasons for these seemingly nonuniform definitions is given by the following theorem:

Theorem In any nonterminal region of length $n_i > 0$, $H_i < L_i$

Proof: First consider a transition region. Since there are no crossunders, the relative positions of the various words are unchanged if the number of left falls equals the number of right falls. In that case, $H_i = L_i$. Before another right crossunder can occur, the right side must drop more than the left, and vice versa. Thus, the theorem is true for transition regions.

By the same argument, we can also show that in any crossunder-less sequence of questions prceding a right crossunder, the number of right falls must exceed (or equal) the number of left falls,

and vice versa. Hence the claim is also true for nontransition regions, since any nontransition region can be subpartitioned up into crossunderless subregions separated by crossunders. Each crossunderless subregion precedes a crossunder in which the light side falls. So in the j^{th} subregion, $H_j \leq L_j$. The crossunders themselves are light falls, incrementing L but not H. q.e.d.

Part 3) Behavior of the averages

Definition: Let $\Delta_i x_{j,k}$ denote the increase in $x_{j,k}$ which occurs during the i^{th} region.

Theorem: In any region of length n_i, $\Delta_i x_{1,3} \geq (n_i + H_i)/3 - 1/3$

Proof:

Left regions and right-left regions: In these regions, no 3,4 crossunders occur, and the left side is light. Throughout the region, $x_{1,3}$ increases by 1/3 iff the light side falls and by 2/3 iff the heavy side falls.

$$\Delta_i x_{1,3} = (L_i + 2H_i)/3 = (n_i + H_i)/3$$

Left-right regions: Similarly, in a left-right region

$$\Delta_i x_{1,3} = (n_i + L_i)/3 \geq (n_i + H_i)/3$$

Equality occurs here iff $n_i = L_i = H_i = 0$

Right regions: In right regions, $\Delta_i x_{1,5}$ and $\Delta_i x_1$ are easily computed

$$\Delta_i x_1 = H_i$$

$$\Delta_i x_{1,5} = (2n_i + H_i)/5$$

The averages are related by the equations

$$3\, x_{1,3} = x_1 + 2\, x_{2,3}$$

$$5\, x_{1,5} = 3\, x_{1,3} + 2\, x_{4,5}$$

$$x_{1,3} = 5/6\, x_{1,5} + 1/6\, x_1 - (x_{4,5} - x_{2,3})/3$$

Both boundaries of a right region occur just before or after a 3,4 crossunder. At the boundaries, from Fig. 3-7,

$$0 \leq x_{4,5} - x_{2,3} \leq 1$$

The increase in $x_{1,3}$ is its difference between the two boundaries.

$$\Delta_i x_{1,3} \geq (n_i + H_i)/3 - 1/3$$

Part 4) Slack, bounding the number of regions

Intuitively, slack is the amount that x_2 and x_3 can rise and fall between hitting x_1 and $x_{4,5}$. Formally, we shall have occasion to use either of the two following definitions:

$$s = (x_4 - x_3) + (x_2 - x_1)$$

$$s' = x_{4,5} - x_1$$

It is clear that these two definitions are approximately equal.

$$|s - s'| \leq 3/2$$

Slack does not change except at crossunders. During a transition region, slack stays constant. In a right-left transition region, $(x_2 - x_1)$ decreases to zero, but $(x_4 - x_3)$ increases. At the start of such a region, $0 \leq (x_4 - x_3) \leq 1$. In a left-right transition region, the roles of $(x_2 - x_1)$ and $(x_4 - x_3)$ are interchanged. In either case, if we let s denote the slack during the transition region R_i, we have

$$H_i + s \leq L_i \leq H_i + s + 1$$

At a crossunder, slack can only increase. s' increases by at least 1/2 at each crossunder. (See Figure 3-7). Between every two left-right regions, there is at least one left region and at least one right region, so s' increases by at least one unit. Consequently, in the k^{th} left-right region, $s \geq k-3/2$

$$n_k \geq H_k + L_k \geq 2H_k + s \geq k - 3/2.$$

Let K-1 be the total number of left-right regions. Summing the lengths of all of them gives (recalling that at least one right region and one left region [both nonempty] occur between any two left-right regions)

$$N > \sum_{k=1}^{K-1} n_k \geq \sum_{k=1}^{K-1} (k+1/2) \geq (K-1)/2$$

$$K < (2N)^{1/2} + 1$$

We note that the total number of all types of regions is no more than 4K.

Part 5) Bounding the number of paths(†)

In any region R_i, there are certainly no more than $\binom{n_i}{H_i}$ paths which have the parameter H_i. Actually, there are usually far fewer. Most patterns of H_i falls of the heavier side of the partition would violate the boundary conditions on the region R_i. Nevertheless, $\binom{n_i}{H_i}$ is an upper bound. The total number of paths having given sets H_i and n_i is bounded by

$$\prod_{i=1}^{4K} \binom{n_i}{H_i}$$

In order to find the total number of paths which have a given $H = \Sigma H_i$, and a given $N = \Sigma n_i$, we must sum this product over all decompositions of H and N into no more than 4K parts. This results in a double sum. For any fixed decomposition of N, the sum over all decompositions of H is given by

(†) The reader may be tempted by the direct argument that at each step, either the light side can fall or the heavy side can fall. Over all N questions, this can happen $\binom{N}{H}$ ways. Unfortunately this argument is invalid, because a given set of "heavy" falls may correspond to several paths. Until the regions are specified, the relationship between paths and sequences of lights and heavies is <u>not</u> 1 to 1.

$$\sum_{\Sigma H_i = H} \binom{n_i}{H_i} = \binom{N}{H}$$

Finally, the number of decompositions of N into at most 4K parts is given by (using Sterling's inequality (1730)†)

$$\sum_{k=0}^{4K} \binom{N}{k} = \binom{N}{4K} = \frac{N^{4K}}{(4K)!} < (e^2 N/32)^{2(2N)^{1/2}} \text{ for } K < (2N)^{1/2}$$

We observe from the first four parts of this proof that the probability of error for any path with given H is

$$\leq (q/p)^{4K/3} \; p^{(N+H)/3} \; q^{N - (N + H)/3} \quad , \text{ with}$$

strict inequality unless perhaps if there are no left-right transitions of non-zero length.

Combining this with the result of the last section,

$$P_e \leq \left((q/p)^{1/3} \; (e^2 N/32)^2\right) \; ((2N)^{1/2} + 1) \; (p^{1/3} q^{2/3} + p^{2/3} \; q^{1/3})^N$$

Conclusions about 5 codewords

From the results of parts 3) and 4), we note that the paths which make a significant contribution to the probability of decoding error are those for which no significant fraction of the block is spent in left-right transition regions. During the first few questions, almost anything can happen. After that, however, Nature must get down to business to clobber Coder. For a while, Nature allows x_1 to rise considerably above $x_2, \ldots x_5$. This is a right region. Then Nature abandons x_4 and x_5, and lets x_1 gradually sink back to x_2 and x_3. This is a right-left transition region. Finally x_1 meets x_2 and x_3, and from then on, Nature keeps all three top words together, causing a final left region.

The two extreme cases of this strategy are essentially the same as those shown in Figures 3-5 and 3-6, with $x_{2,3}$ replacing x_2 and $x_{4,5}$ replacing x_3. In Figure 3-5, the final left region occupies almost the entire block; in Figure 3-6, the initial right region occupies 2/3 of the block; the right-left transition

(†) Details are given on p. 216 of Fano (1961).

region, 1/3; and the final left region is virtually nonexistent.

The strategy which plays W_1, W_3, and W_5 against W_2 and W_4 can be analyzed in a similar manner. This strategy also results in an exponentially optimum error probability.

EXTENSION TO M CODEWORDS

In this section we extend the results of the previous section to the case of M codewords, where M is any finite number. This is the strategy we shall use:

W_1

W_2W_3

W_4W_5

W_6W_7

W_8W_9

...

We again note that adjacent pairs of words will remain together. For any k, after any number of questions have been asked,

$$x_{2k} \leq x_{2k+1} \leq x_{2k} + 1$$

We again distinguish two possible types of crossunders. Left crossunders occur when, for some i, $x_{4i+1} = x_{4i+2}$ and the left side of the partition then falls, necessitating an interchange of labels among W_{4i+1} and W_{4i+2} (and possibly also W_{4i} and/or W_{4i+3}). Right crossunders occur when, for some i, $x_{4i+1} = x_{4i}$ and the right side of the partition then falls, necessitating an interchange of labels among W_{4i-1} and W_{4i} (and possibly also W_{4i-2} and/or W_{4i+1}). If all the words whose labels change are among the set W_{2i-1}, W_{2i}, W_{2i+1}, W_{2i+2}, for some one particular i, then this crossunder is called a <u>single crossunder</u>; if not, it is called a <u>multiple crossunder</u>. For example, W_1 may cross under W_2 on the same question that W_5 crosses under W_6.

Another peculair type of crossunder occurs when, for some i, x_{2i+1} crosses under x_{2i+6}. We call these <u>degenerate crossunders</u>. Prior to a degenerate crossunder, $x_{2i+1} = x_{2i+2} = x_{2i+3} = x_{2i+4} = x_{2i+5} = x_{2i+6}$. At the crossunder x_{2i+5} also crosses under x_{2i+6}, so every degenerate crossunder is also a multiple crossunder. The converse statement is not true.

Degenerate crossunders are unusually nasty, in that none of the averages is well-behaved. For example, if x_1 crosses under x_6, then $x_{1,3}$ does not increase at all. During the first part of the block, every crossunder is a degenerate crossunder. However, if $M << N$, then eventually degenerate crossunders cease. None occur toward the end of the block. In fact, all degenerate crossunders generally occur consecutively.

At any positive rate, degenerate crossunders occur at every question. x_1, x_2, and x_3 may cease to be involved in these degenerate crossunders, but $x_{M/2}$ continues to misbehave. x_1 may dive back down into the pack of other codewords beneath it and again suffer degenerate crossunders.

We postpone further investigation of degenerate crossunders until Chapter 4. Here we circumvent the problem by assuming that all pairs of words are separated when we start:

$$x_1 < x_{2,3} < x_{4,5} < \cdots < x_M$$

This assumption is no restriction iff $M << N$. In that case we can afford to play favorties by arbitrarily biasing various codewords with up to M votes initially. Since each word will receive a fraction of N (generally between N/3 and 2N/3) negative votes by the end of the block, the relatively insignificant initial bias cannot exponentially effect the probability of error.

Since there are no degenerate crossunders, the averages $x_{1,4i+1}$ are well-behaved except at left crossunders; the averages $x_{1,4i-1}$ are well-behaved except at right crossunders. We will

again be able to define a heavy side and a light side of the partition in each region, such that the increase in the averages can be calculated.

Our method of establishing the exponential optimality of this strategy is the same as the previous section. However, additional complications force us to modify sections 1), 3), and 4). We give the necessary modifications and certain collateral results in Parts 1'), 3'), and 4'). Parts 2) and 5) apply without essential changes.

Part 1') Partitioning the block into well-behaved regions

Although the plot here is basically the same as Part 1), the details are more complicated. For one thing, we distinguish among many subtypes of the four basic types of regions.

A 2i-1,2i region is internally bounded on each side by a 2i-1,2i crossunder. Although this region may contain many 2i-1,2i crossunders, it contains no 2j-1,2j crossunders for any $j < i$ or for $j = i+1$.

If i is odd, a 2i-1,2i region is a left region; if i is even, it is a right region.

A 2i-1,2i;2i+1,2i+2 increasing transition region follows a 2i-1,2i region and precedes a 2i+1,2i+2 region. A 2i+1,2i+2;2i-1,2i decreasing transition region follows a 2i+1,2i+2 region and precedes a 2i-1,2i region. Neither of these transition regions contain any 2j-1,2j crossunders for any $j \leq i+1$. Both increasing and decreasing transition regions are subclassified as right-left and left-right regions, depending on whether the preceding region is right and the following region is left or vice versa.

The first 2i+1,2i+2;2i-1,2i decreasing transition region that eventually follows a given 2i-1,2i;2i+1,2i+2 increasing transition region is called its compensating region. Likewise the last 2i-1,2i; 2i+1,2i+2 increasing transition region before a given 2i+1,2i+2; 2i-1,2i decreasing transition region is called its compensating region.

We shall see that transition regions occur in compensating pairs. A compensating pair of transition regions corresponds to a mated pair of parentheses. Increasing transition regions act as left parentheses; decreasing transition regions act as right parentheses. Notice that any pair of compensating regions consists of one left-right region and one right-left region.

If the first crossunder of the block is a 3,4 crossunder, the first 3,4;1,2 transition region does not have a preceding compensating region in the normal sense. In this exceptional case, we assume that an empty 1,2;3,4 transition region precedes the first question of the block. This is equivalent to assuming that the last crossunder before the block started (an obviously hypothetical notion) was a 1,2 crossunder. As in Part 1), we also introduce here the additional assumption that a 1,2 crossunder would occur next if the block were extended beyond the final question. This assumption avoids the ambiguities that would otherwise arise in the partitioning of the lattermost part of the block.

To partition the path into regions we first locate all 1,2 regions, then all 3,4 regions, then all 1,2;3,4 and 3,4;1,2 regions, then all 5,6 regions, then all 3,4;5,6 and 5,6;3,4 regions,... until all questions belong to some well defined region. A formal program for doing this is given on the following page; an example, on the page after that.

The example given in Figure 3-8 is hypothetical in that it assumes a sequence of crossunders which might well be impossible in any actual path. The partitioning process as stated on the next page can be applied to any sequence of crossunders, even such hypothetical ones.

PROGRAM FOR PARTITIONING ANY GIVEN PATH INTO REGIONS

Initialization: Annex 1,2 crossunders just before the beginning and just after the end of the block.

1,2 regions: Locate all 1,2 crossunders and all 3,4 crossunders. Each cluster of 1,2 crossunders not containing any 3,4 crossunders is placed within a 1,2 region. Then with i = 1,

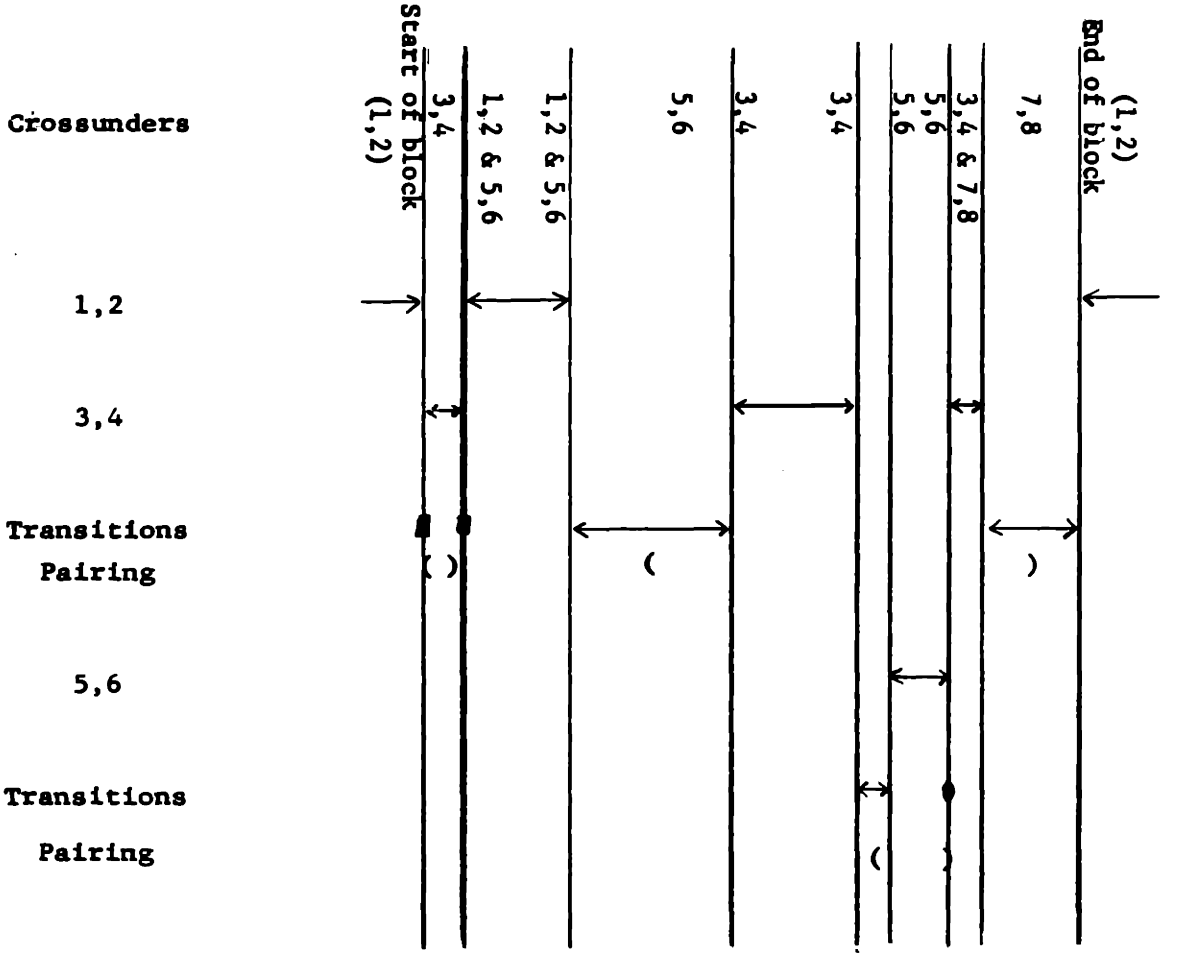
Loop: 2i+1,2i+2 regions: Consider only the as-yet-undefined regions, which will be denoted by $R_k^{2i-1,2i}$. Each such region lies between two 2i-1,2i regions. It contains no 2j-1,2j crossunders for any j $\leq$ i, but it does contain at least one 2i+1,2i+2 crossunder. Locate all 2i+1,2i+2 crossunders and 2i+3,2i+4 crossunders in $R_k^{2i-1,2i}$. Each cluster of 2i+1,2i+2 crossunders not containing any 2i+3,2i+4 crossunders is placed within a 2i+1,2i+2 region.

Transition regions: The preceding step resulted in at least one (and possibly more) 2i+1,2i+2 regions in each region $R_k^{2i-1,2i}$. That part of $R_k^{2i-1,2i}$ preceding its first 2i+1,2i+2 region within it is taken as a 2i-1,2i;2i+1,2i+2 increasing transition region; that part of $R_k^{2i-1,2i}$ following its last 2i+1,2i+2 region within it is taken as a 2i+1,2i+2; 2i-1,2i decreasing transition region. (Either or both of these transition regions may conceivably be empty.) These two transition regions form a compensating pair.

If all regions are now defined the partitioning process is finished. If there remain any undefined regions, each lies between two 2i+1,2i+2 regions. Increase i by one and return to LOOP.

End of program

Figure 3-8 PARTITIONING A HYPOTHETICAL PATH INTO REGIONS



We note at this point that there are several other ways of defining the regions which lead to similar proofs of the exponential optimality of this sections's order strategy for M codewords. Among these alternate definitions, the simplest merely lumps together each 4,5;6,7 regions with its corresponding 6,7;4,5 region and all they enclose into a single deep region. According to that system of classification, there are only five types of regions: 1,2 regions, 3,4 regions, 1,2;3,4 regions, 3,4;1,2 regions, and deep regions.

The more detailed classification programmed on the preceding page has the advantage that it leads to certain collateral results which provide additional insight into the behavior of the order strategy. It is possible to analyze the structure of the deeper regions in more detail. The most enlightening theorem in this direction is the following

Theorem:(†) Between any two questions in a 2i-1,2i region,

$$x_{2i,2i+1} - x_{2i-4,2i-3} < x_{2i-2,2i-1} - x_{2i-6,2i-5} \leq \cdots$$
$$\leq x_{2j,2j+1} - x_{2j-4,2j-3} \leq x_{2j-2,2j-1} - x_{2j-6,2j-5} \leq \cdots$$
$$\leq x_{8,9} - x_{4,5} \quad \underline{<} \; x_{6,7} - x_{2,3} \leq x_{4,5} - x_1 \qquad \text{for } i \geq j+2 \geq 8$$

For example, a typical spacing of words in a 9,10 region is

x_1

$x_{2,3}$

$x_{4,5}$

$x_{6,7}$

$x_{8,9}$

$x_{10,11}$

...

(†) The proof of the exponential optimality of the order strategy for M codewords does not depend on this collateral theorem. Readers interested only in that major result may skip at once to Part 3').

Proof: For any $j < i$, there is a compensating pair of 2j-1,2j;2j+1, 2j+2 and 2j+1,2j+2;2j-1,2j transition regions which surround the given 2i-1,2i region. Throughout these transition regions and all the regions they enclose there are no 2k-1,2k crossunders for any $k \leq j$. Immediately preceding the 2j-1,2j; 2j+1,2j+2 transition region is a 2j-1,2j region ending with a 2j-1,2j crossunder. At the boundary between these two regions, $x_{2j+1} = x_{2j-2} + 1$ (†) (If unclear on this points, review Figure 3-7.) At the boundary,

$$x_{2j-2,2j-1} - x_{2j-6,2j-5} \geq x_{2j,2j+1} - x_{2j-4,2j-3} - 1$$

with equality iff

$$x_{2j-6} = x_{2j-5} = x_{2j-4} = x_{2j-3}$$

and

$$x_{2j-2} = x_{2j-1} = x_{2j} - 1 = x_{2j+1} - 1$$

Immediately following the 2j-1,2j;2j+1,2j+2 transition region is a 2j+1,2j+2 crossunder. This crossunder decreases $x_{2j,2j+1} - x_{2j-4,2j-3}$ by either 1/2 or 1, accordingly as $x_{2j+1} = x_{2j+1}$ or $x_{2j+1} = x_{2j}$, just before the crossunder occurs. In either case, immediately following the crossunder,

$$x_{2j-2,2j-1} - x_{2j-6,2j-5} \geq x_{2j,2j+1} - x_{2j-3,2j-4}$$

Further crossunders can only further decrease the right side, so the inequality remains valid at least until the next 2j-1,2j region.

This proves all of the inequalities claimed in the theorem with the possible exception of the first. To prove this, we note that any point in the 2i-1,2i region lays between two 2i-1,2i crossunders. Immediately preceding the crossunder following the point in question,

$$x_{2i} = x_{2i-1} \quad \text{and } x_{2i-4} > x_{2i-5}$$

(†) To include the exceptional case that j=1, we may have to interpret x_0 to mean x_1.

These imply

$$x_{2i-3} > x_{2i-6} \quad \text{and} \quad x_{2i+1} \leq x_{2i-2} + 2$$

Hence

$$x_{2i-2,2i-1} - x_{2i-6,2i-5} \geq x_{2i,2i+1} - x_{2i-4,2i-3}$$

with equality iff

$$x_{2i+1} - 1 = x_{2i} = x_{2i-1} = x_{2i-2} + 1$$

and

$$x_{2i-6} = x_{2i-5} = x_{2i-4} + 1 = x_{2i-3} + 1$$

The former condition is an impossibility, for it implies that $x_{2j+1} \neq x_{2j}$; $x_{2j-1} \neq x_{2j\pm2}$ following the previous 2j-1,2j crossunder. This contradicts the fact that $x_{2j+1} = x_{2j-2} + 1$ following any nondegenerate 2j-1,2j crossunder. Hence we have strict inequality of the claim just before the next crossunder following the point in question. Since neither side of the inequality can change except at crossunders, the inequality is valid between any two questions in a 2i-1,2i region.

q.e.d.

Part 3') Behavior of averages

<u>Transition regions:</u> In a 2j-1,2j; 2j+1,2j+2 or 2j+1,2j+2;2j-1,2j left-right transition region, there are no confusing crossunders and the right side is light. The increases in the averages are given by

$$\Delta_i x_1 = H_i \qquad \Delta_i x_{1,3} = (n_i + L_i)/3$$

$$\Delta_i x_{1,5} = (2n_i + H_i)/5 \qquad \Delta_i x_{1,7} = (3n_i + L_i)/7$$

$$\cdots$$

$$\Delta_i x_{1,2j+1} = (jn_i + S_i)/(2j+1) \quad \text{where } S_i = H_i \text{ iff } j \text{ even}, \; S_i = L_i \text{ iff } j \text{ odd}$$

In a similar right-left transition region, the left side is light. This gives

$$\Delta_i x_1 = L_i \qquad \Delta_i x_{1,3} = (n_i + H_i)/3$$

etc., as above with L and H interchanged.

In any case,

$$\Delta_i x_{1,2j+1} \geq (jn_i + H_i)/(2j+1)$$

Nontransition regions

In a 2j-1,2j region, there are no 2i-1,2i crossunders for i<j or i = j + 1. This at once implies that the averages $x_{1,2i-1}$ are well-behaved, and are given by the expressions derived above for transition regions. Right regions are like left-right regions (right side light); left regions are like right-left regions (left side light).

The average $x_{1,2j-1}$ is not given by its expression for transition regions, because it is affected by the 2j-1,2j crossunders. However, we can compute this average by relating it to the other averages. We start with three identities, valid anywhere.

$$(2j-1)\, x_{1,2j-1} = (2j-3)\, x_{1,2j-3} + 2\, x_{2j-2,2j-1}$$

$$(2j+1)\, x_{1,2j+1} = (2j-1)\, x_{1,2j-1} + 2\, x_{2j,2j+1}$$

Solving for $x_{1,2j-1}$ gives

$$x_{1,2j-1} = ((2j-3)/2(2j-1))x_{1,2j-3} + ((2j+1)/2(2j-1))\, x_{1,2j+1} - (x_{2j,2j+1} - x_{2j-2,2j-1})/(2j-1)$$

At the ends of a 2j-1,2j region we have 2j-1,2j crossunders, so that $x_{2j,2j+1} - x_{2j-2,2j-1} \leq 1$. This effectively eliminates the last term in the expression for $x_{1,2j-1}$. The averages $x_{1,2j-3}$ and $x_{1,2j+1}$ are well-behaved throughout the region, and their increases across the region are given by the expressions computed for transition regions. Plugging these into the formula for $x_{1,2j-1}$ gives

$$((j-1)n_i + H_i - 1)/(2j-1) \leq \Delta_i x_{1,2j-1} \leq ((j-1)n_i + H_i + 1)/(2j-1)$$

By summing over all regions, we can calculate the increase in the value of an average over the entire block. The average of major concern to us is $x_{1,3}$, which is given by

$$x_{1,3} = \sum_{\text{all regions}} \Delta_i \, x_{1,3} = (N+k)/3 \quad \text{where}$$

$$k = \sum_{\substack{\text{left regions} \\ \& \text{ right-left regions} \\ \& \text{ 4,5 regions}}} H_i + \sum_{\substack{\text{left-right regions} \\ \& \text{ deep regions}}} L_i \pm \epsilon/3$$

where $\epsilon \leq$ number of 4,5 regions. We shall see in Part 4') that the nondegenerate assumption introduced at the beginning of this section (just before Part 1') enables us to claim that every transition region is nonempty. This includes the transition regions preceding 4,5 regions. In each such transition region, $H_i < L_i$. The excess introduced in these regions more than makes up for ϵ, and we have

$$k \geq \sum_{\text{all regions}} H_i = H$$

This result will enable us to prove the desired exponential optimality. It also shows that Nature cannot allow any non-zero fraction of the block to be spent in left-right regions or deep right regions without conceding an exponentially smaller probability of decoding error. (For rigorification of this claim, one needs to invoke a theorem on increasing slack which will appear in Part 4'.)

In order to reach conclusions about the overall increase in the other averages, one must subpartition the shallower regions according to the crossunders of the desired averages. The details are straightforward and will be omitted. From the above computations one then deduces the following general results for the overall increase in the averages during the entire block.

$$x_{1,3} \geq (N+H)/3$$

$$x_{1,5} \geq (2N+H)/5$$

$$x_{1,7} \geq (3N+H)/7$$

$$x_{1,2j+1} \geq (jN+H)/(2j+1)$$

This furnishes additional insight into the types of errors possible. We see that successive higher pairs of words tend to end lower and lower. Thus, although $x_{1,3}$ might be as little as N/3, $x_{1,5}$ must be at least 2N/5. This leads us to the conclusion that even when the top three words end in a tie, all the rest of the words must end up with almost N/2 (or more) votes against them.

Part 4') Bounding the number of regions

The basic goal here is to show that the words spread out sufficiently far sufficiently fast, so that the result of Part 5 is still exponentially valid. We strive for a considerably stronger result than completely necessary. We shall show that even if one considers <u>all</u> crossunders (including those with very high subscripts, which usually are buried unnoticed in the shallower regions when the block is partitioned according to the program given in Part 1'), successive clusters of right and left crossunders must be separated by longer and longer transition regions.

Intuitively, we can consider the two sides of the partition as two intermeshed combs:

x_1

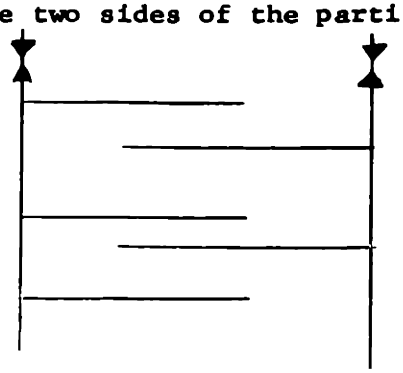
$x_{2,3}$

$x_{4,5}$

$x_{6,7}$

$x_{8,9}$

...



We pick up the combs by the handles as shown. Suppose we bashed the combs back and forth several times, and that every time two opposite teeth hit, they bent (permanently) by an amount Δ. It is intuitively obvious that if we bashed the combs back and forth enough times, we could eventually accumulate as much slack as we desire. (Slack is the amount we can move the combs between pushing until some teeth hit and pulling until some other teeth hit.)

Unfortunately, attempts to rigorify this intuitive formulation are fraught with difficulties. Starting in the obvious manner, we define slack between the two sides of the partition by

$$s = \min_i (x_{4i} - x_{4i-1}) + \min_j (x_{4j-2} - x_{4j-3})$$

or alternatively

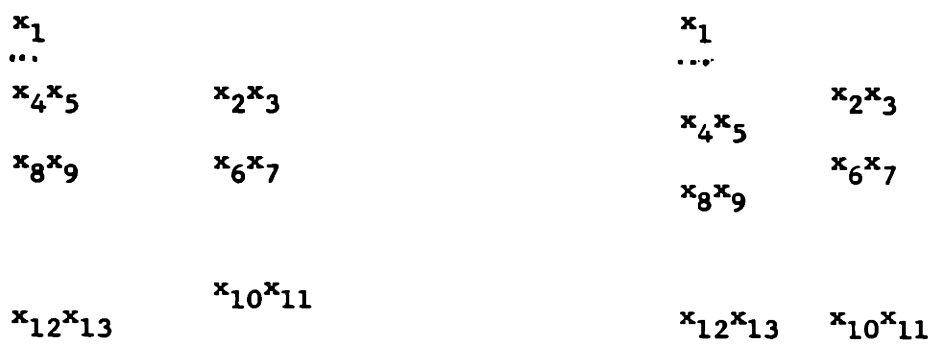
$$s' = \min_i (x_{4i,4i+1} - x_{4i-2,4i-1}) + \min_j (x_{4j-2,4j-1} - x_{4j-4,4j-3})$$

(To include the possibility that $4j-4 = 0$ in this last subscript, we conventionally define $x_{0,1} = x_1$).

Degenerate crossunders cannot occur unless the slack is 0.

False Conjecture: From any "conceivable" position, slack cannot decrease. Here conceivable may be defined in any way which admits the following counterexample. It remains open to question whether or not it is possible to reach such a position from a given initial position.

Counterexample: Before right falls to After



Before, $s = s' = (x_4 - x_3) + (x_6 - x_5) = 0 + x_6 - x_5$

After, $s = s' = (x_{12} - x_{11}) + (x_6 - x_5) = 0 + x_6 - x_5$

The slack decreased by one unit.

This counterexample places in evidence the type of Diophantine problems that plague us here. They are very similar to the problems encountered in the proof of the deep region theorem of Part 1').

To show that this behavior is indeed locally eccentric, and does not invalidate our intuition, we prove the following

Theorem: Slack can never decrease by more than one unit. If it does decrease at some particular crossunder, then it increased on the immediately previous crossunder, and it must also increase on the immediately following crossunder. In other words, over pairs of crossunders, slack is monotonic nondecreasing.

Proof: We prove only part of the claim, namely that the next crossunder results in an increase. The proof that the previous one also did is similarly tedious and unenlightening. The skeptical reader can readily construct the proof for himself along lines similar to that given here.

If the next crossunder is the same direction as the nasty one, there is no problem. During two consecutive crossunders of the same direction, all words on the falling side of the partition fall either one unit or two units; all words on the stationary side fall either zero units or one unit. At the start of the two consecutive (same direction) crossunders, one of the minimums is zero. (We are using s, rather than s', as the definition of slack.) That minimum cannot further decrease. The other minimum is the difference between a word on the falling side and a word on the stationary side. But all words on the falling side fall by at least one unit, which is as much as any words on the stationary side. So this minimum cannot decrease either. This verifies the case when both crossunders are in the same direction.

In order for the slack to decrease at a single crossunder,

the zero minimum must remain zero and the other minimum must decrease. This decrease can occur only if it is the difference between a word on the falling side which remains stationary and a word on the stationary side which falls. If the minimum was degenerate, all pairs of adjacent words which were equal to the minimum must behave in this same way. Thus there is no loss in generality in assuming that the minimum was unique, say $x_{2k} - x_{2k-1}$. We further note that the only possibility is $x_{2k} = x_{2k+1}$; $x_{2k-1} = x_{2k-2}$ just after the nasty transition. At this point $x_{2k+2} - x_{2k+1} = x_{2k-2} = x_{2k-3}$. However, some other $x_{2j+2} - x_{2j+1} = 0$, where j and k have the same parity mod 2 (i.e., these differences are in the same direction).

If the next crossunder is of the opposite direction, it occurs between x_{2k} and x_{2k-1}. At the crossunder, their difference goes from zero to one. The other minimum comprising the slack is $x_{2j+2} - x_{2j+1}$, which cannot decrease at this crossunder. Hence the second crossunder increases the slack.

q.e.d.

Having sampled the tedious labor apparently required to rigorify even the simplest and most obvious theorems of this type, we will omit the proof of the next theorem.

Theorem: Given M codewords with slack s, there exists a function f(M), independent of s, such that the slack will be increased by any sequence of crossunders which alternates direction f(M) or more times.

Conjecture: $f(M) = [(M-1)/4]$

The worst case seems to be the situation in which all the differences are equal in both of the minimums defining the slack.

Concluding as in Part 4),

$K \leq (2f(M)N)^{1/2}$ bounds the total number of transition regions of either type. For large $N >> M$, $N >> f(M)$, K is negligible compared to N. Thus the results of Part 5) still apply.

GENERALIZATION TO SYMMETRIC BINARY-INPUT CHANNELS

Symmetric binary-input channels were first considered by Dobrushin (1962). Such channels are symmetric in the sense that, if the outputs are numbers numbered such that $P_{1,1} \geq P_{2,1} \geq \cdots \geq P_{j,1} \geq \cdots \geq P_{J,1}$, then

$$P_{j,2} = P_{J+1-j,1} \quad \text{for all } j = 1, \ldots J$$

We may take this as the definition of a symmetric binary-input channel.

We will outline here the straightforward but tedious method by which the results of the previous sections for 3 codewords, 5 codewords, and M codewords may be generalized from the BSC to the class of symmetric binary-input channels.

Instead of considering the number of votes against a particular codeword, we consider the logarithm of the probability of the received output sequence under the assumption that a particular codeword was the selected message. The decoder computes this quantity for each word as the game progresses. The trajectories of these functions correspond to the trajectories plotted in Figures 3-4.

The codewords may still be ordered according to their rankings as computed by this function, and the order strategy which plays the most probable word with the fourth, fifth,... words against the second, third,... words may still be used. Whenever a digit is received, both partitions generally fall, but one will fall more than the other. Some received symbols (approximately equiprobable from both inputs) will cause both sides of the partition to fall about the same amount.

Although it is no longer true that $x_3 \leq x_2 + 1$, it is possible to find some number δ such that $x_3 \leq x_2 + \delta$. (†)

(†) Such a δ cannot be defined for channels which have $P_{1,2} = P_{J,1} = 0$ but the result can be extended to these channels by a simple auxiliary argument.

δ is a function only of the channel, and does not depend on the number of questions already asked or the number of questions remaining.

The number of crossunders can still be bounded as in Part 4'). One can still define a heavy side and a light side of the partition within any given region. Instead of the number of heavy falls and the number of light falls, H_i and L_i now become vectors $\underline{H}_i$ and $\underline{L}_i$, whose components count the number of times that the heavy side fell by the various possible amounts. The averages within any given region may then be bounded by a manner analagous to Part 3'), and the total number of paths may be bounded as in Part 5'). The calculations are complicated by the presence of multinomial coefficients instead of binomial coefficients.

The result that one obtains in this manner is that, for any symmetric binary input channel,

$$F_\infty = F_3 = -\ln \sum_j p_{j,1}^{1/3} p_{j,2}^{2/3} = u_{1,2}(1/3)$$

THE BINARY ASYMMETRIC CHANNEL

We close this chapter with an investigation of the binary asymmetric channel of Figure 2-3. This channel enables us to proceed with our arguments without the obscuring complications of multinomial coefficients which one encounters with multioutput channels, yet this channel is sufficiently complicated that we are unable to determine F_∞. We shall show only that the best order strategy is unable to attain the exponent E_2. Our arguments, as stated here, are not completely rigorous, but they could be made so by sufficiently elaborate calculations.

As in the previous section, we consider the logarithm of the probability of the received sequence, under the hypothesis that a particular word is the message. We plot this trajectory for each codeword.

We start with a code containing M codewords (M small), We use an order strategy which plays the most probable word on the input a_2, and all the other (M-1) words on the input a_1. Let k be the number of received b_1's. Then a typical plot of the trajectories might be as shown in Figure 3-9.

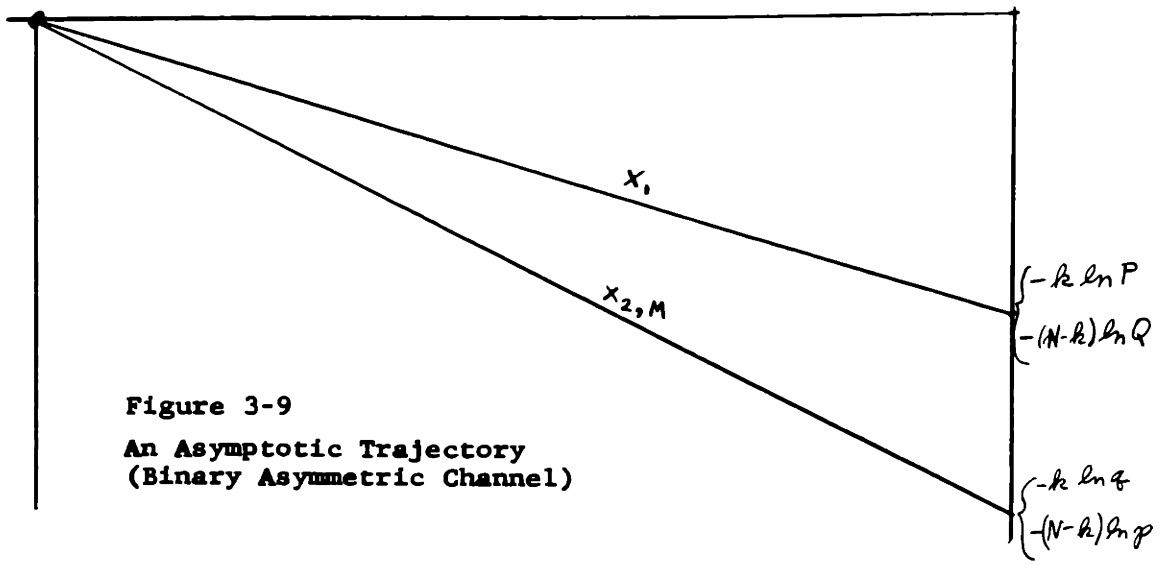


Figure 3-9

An Asymptotic Trajectory
(Binary Asymmetric Channel)

There is a critical value of k, given by K ln P + (N-K) ln Q = K ln q + (N-K) ln p

$$\text{or} \qquad K/(N-K) = \frac{\ln (Q/p)}{\ln (q/p)} < 1 \qquad (3.901)$$

We write

$$P_e \text{ "=" } \sum_{k<K} \binom{N}{k} q^k p^{N-k} + \sum_{k>K} \binom{N}{k} \left[q^{(M-1)/M} p^{1/M}\right]^k \left[Q^{1/M} p^{(M-1)/M}\right]^{N-k} \qquad (3.902)$$

where the "=" means equal in exponent as N goes to infinity.

The justification of this claim is as follows: For all $k/N < K/N$ the top word stays above the others almost the entire block length. In fact, it can crossunder only a finite number of times. In the other case, when $k/N > K/N$, then asymptotically, crossunders must occur frequently, and in fact all M words will end approximately tied. More precisely, one can show that the deviation of any of the words from the average of all words is a term which behaves as $N^{1/2}$.

The terms in the above sum are plotted in Figure 3-10

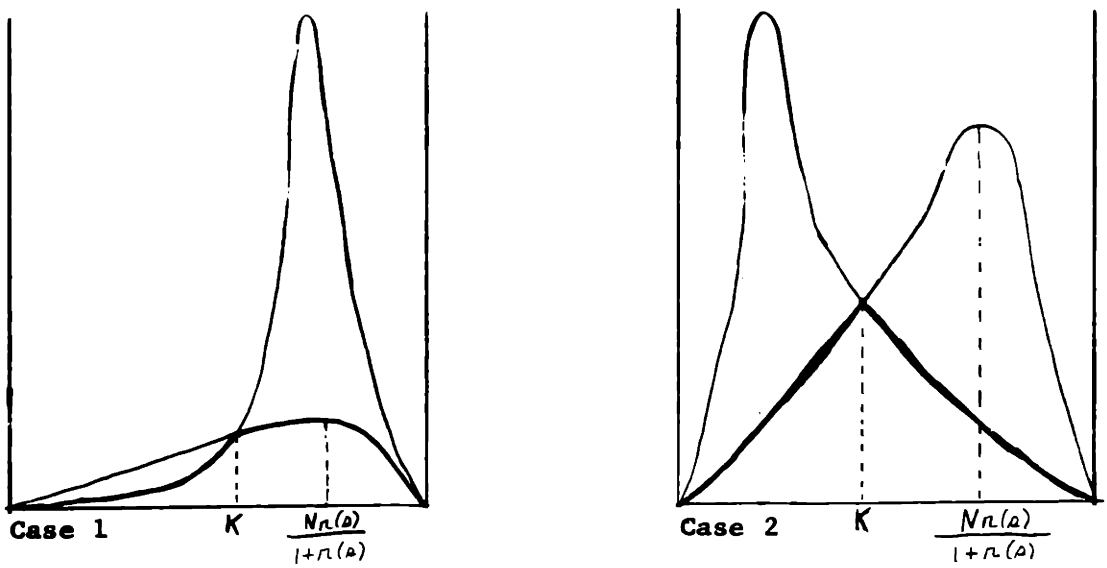


Figure 3-10 The Terms of (3.902) vs k

To evaluate the above expression for P_e, we consider the two sums separately. If the first sum is taken over all the terms, its value is 1. The dominant term occurs when k/(N-k) = q/p.

Next we consider the sum

$$\sum_k \binom{N}{k} (q^s p^{1-s})^k (Q^{1-s} p^s)^{N-k} = (q^s P^{1-s} + p^s Q^{1-s})^N \tag{3.903}$$

The dominant term is given by

$$k/(N-k) = q^s P^{1-s}/Q^{1-s} p^s = r(s) \text{ by definition.} \tag{3.904}$$

The function r(s) is monotonic increasing in s, and convex downward. It takes values from P/Q to q/p as s varies from 0 to 1. A plot of r(s) is given in Figure 3-11.

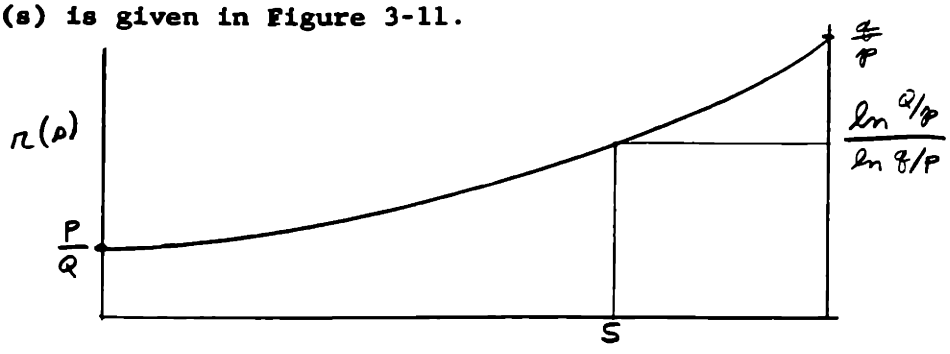


Figure 3-11 The Function r(s) vs s

We next note that there exists some particular value of s, denoted by S, for which K/(N-K) = r(S). This follows from the fact that

$$P/Q < \ln (Q/P) / \ln (q/P) < q/P \tag{3.905}$$

To prove the left side, we reduce it to

$$H(P) \overset{?}{<} -P \ln q - Q \ln p \tag{3.906}$$

For fixed P and A, the right side of (3.906) attains its unique minimum when q = P; p = Q. That case is outlawed as it reduces the channel to a degenerate one with zero capacity. In all other cases, the inequality holds. The right side of (3.905) can be similarly proved.

Returning now to (3.902), we find two possibilities, as graphed in Figure 3±10.

In Case 1, the dominant term occurs when $k/(N-k) = r(s) > \ln(Q/p) / \ln(q/P)$, with $s = 1 - 1/M$

In this case the dominant error pattern involves frequent crossunders, and the probability of error is given by

$$P_e \doteq \left(r(1-1/M)\right)^N \tag{3.907}$$

In Case 2, the dominant term occurs at the kink between the two expressions, when $k = K$ as defined by (3.901). In this case there are dominant error patterns which have no crossunders at all. The probability of error is given by

$$P_e \doteq \binom{N}{K} q^K p^{N-K} = \binom{N}{K} p^K Q^{N-K} \tag{3.910}$$

Its exponent is given by $E = -K/N \ln[q/(K/N)] - (1-K/N) \ln[p/(1-K/N)]$ (3.911)

$$= -K/N \ln[P/(K/N)] - (1-K/N) \ln[Q/(1-K/N)] \tag{3.912}$$

where

$$K/N = 1 / [1 + (\ln q/P)/(\ln Q/p)] \tag{3.913}$$

$$(N-K)/N = 1 / [1 + (\ln Q/p)/(\ln q/P)] \tag{3.914}$$

so the exponent of (3.910) is given by

$$E = \frac{- \ln[q(1+(\ln q/P)/(\ln Q/p)]}{1 +[(\ln q/P)/(\ln Q/p)]} \quad \frac{- \ln[p (1+(\ln Q/p)/(\ln q/P)]}{1 + [(\ln Q/p)/(\ln q/P)]} \tag{3.920}$$

$$= \frac{- \ln[P(1+(\ln q/P)/(\ln Q/p)]}{1 + [(\ln q/P)/(\ln Q/p)]} \quad \frac{- \ln[Q (1+(\ln Q/p)/(\ln q/P)]}{1 + [(\ln Q/p)/(\ln q/P)} \tag{3.921}$$

Since these two expressions for E are equal, we may interpolate linearly between them and get

$$E = \frac{-\ln[q^x P^{1-x}(1+(\ln q/P)/(\ln Q/p))]}{1+[(\ln q/P)/(\ln Q/p)]} \quad \frac{-\ln[p^x Q^{1-x}(1+(\ln Q/p)/(\ln q/P))]}{1+[(\ln Q/p)/(\ln q/P)]} \tag{3.922}$$

The value of E here is independent of x, so x may be arbitrarily set to whatever value most simplifies any particular computation.

We next compare this result with Gallager's expression for E_2

$$E_2 = \max_{0\le s\le 1} -\ln\left(\sum_j p_{j,1}^{s}\, p_{j,2}^{1-s}\right) \tag{2.08}$$

Differentiating the inner expression reveals that, at the maximum,

$$q^s P^{1-s} / p^s Q^{1-s} = (\ln Q/p)/(\ln q/P) \tag{3.925}$$

This equation can be solved for s, but such a step is tedious and proves unnecessary. Instead, we may manipulate directly with the expression for E_2. From the identity, that

$$1/(1+x) + 1/(1+x^{-1}) = 1 \tag{3.926}$$

we have

$$E_2 = \max_s \frac{-\ln[q^s P^{1-s}(1 + p^s Q^{1-s}/q^s P^{1-s})]}{1 + [p^s Q^{1-s}/q^s P^{1-s}]} \quad \frac{-\ln[p^s Q^{1-s}(1 + q^s P^{1-s}/p^s Q^{1-s})]}{1 + [q^s P^{1-s}/p^s Q^{1-s}]} \tag{3.927}$$

Applying (3.925) where applicable reduces the maximand of (3.927) to (3.922), with x replaced by s. But we have observed that this expression is in fact independent of s, so the maximization over this now-extraneous parameter can be ignored.

We have shown that the error exponent for M codewords, played according to the strategy of the top word vs all the others, is given by

$$F_M = \max_{\substack{0\le s\le 1/M \\ \text{or} \\ 1-1/M \le s\le 1}} -\ln\left(q^s P^{1-s} + p^s Q^{1-s}\right)$$

In Case 1, the maximum occurs at $s = 1/M$ or $1-1/M$; in Case 2, the maximum occurs at some interior point.

Let m be the least integer for which $1 - 1/m > s^*$, where $s^* > 1/2$ maximizes the expression for E_2. We have seen that the order strategy which plays the top word against the bottom (m-1) words is limited to an exponent less than E_2. So we instead consider the order strategy which plays the top and bottom words against the middle (m-2) words. But this strategy is also limited to the same exponent, because now, for any value of k, there will be $\binom{N}{k}$ ways (m-1) words end at $-k \ln q - (N-k) \ln p$. If $k < K$, then all words but the bottom word end there; if $k > K$, then all words but the top word end there. In either case, the second word ends there. Thus the probability of error for this strategy is given by

$$F_m^{(\text{order})} = u_{1,2}(1-1/m)$$

where m is the least integer for which $1-1/m > s^* > 1/2$. It is readily seen that no other order strategy for m codewords can do any better.

Whether this limitation applies to all feedback strategies or merely to order strategies is not known.

EXERCISES

Exercise 3-1

Find the necessary and sufficient conditions on the channel probabilities so that the sphere packing bound is completely degenerate, $C = C_o^+$.

Solution (Gallager, 1964):

Condition 1): $p_{j,k} = 0$ or p_j, for all k for which $\bar{r}_k^* > 0$.

Condition 2): $p_j \exp -C = \sum_k P_k^* p_{j,k}$ for all j.

C is the capacity, given by $C = \ln \sum_j p_j$

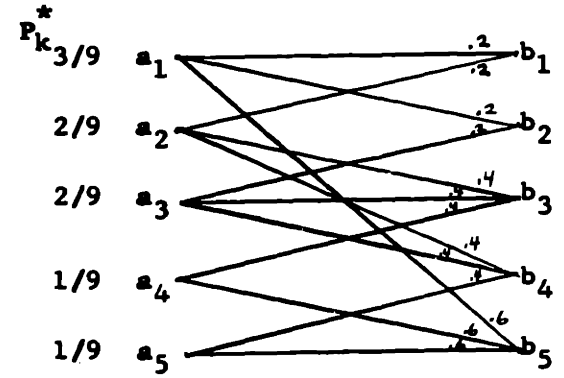
Exercise 3-2

Show by example that P_k^* may depend on k and p_j may depend on j, even though $0 = C_o < C_o^+ = C$.

Solution:

$C_o = 0$;

$C = C_o^+ = \ln 1.8$

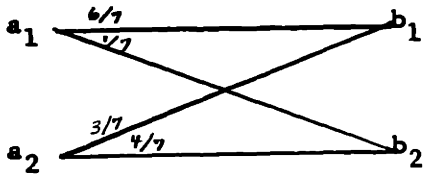


Exercise 3-3

Show that, for M=2 and N=3, it is possible to do better with feedback than without feedback on the following channel. Does this contradict the result that $E_2 = F_2$?

M=2

N=3



Solution: Since $3 << \infty$, this result is not inconsistent with $E_2 = F_2$.

Without feedback, the best code is $\underline{x} = a_1a_1a_1$; $\underline{x}' = a_2a_2a_2$

	$\Pr(\underline{y}/\underline{x})$	$\Pr(\underline{y}/\underline{x}')$
1 term	$\Pr(b_1^3/a_1^3) = 216/343$	$\Pr(b_1^3/a_2^3) = (27/343)$
3 terms	$\Pr(b_1^2b_2/a_1^3) = 36/343$	$\Pr(b_1^2b_2/a_2^3) = (36/343)$
3 terms	$\Pr(b_1b_2^2/a_1^3) = (6/343)$	$\Pr(b_1b_2^2/a_2^3) = 48/343$
1 term	$\Pr(b_2^3/a_1^3) = (1/343)$	$\Pr(b_2^3/a_2^3) = 64/343$

The probability of error may be computed from the formula

$$P_e = 1/2 \sum_{\underline{y}} \min_{\underline{v}=\underline{x} \text{ or } \underline{x}'} \Pr(\underline{y}/\underline{v})$$

These minimum terms have been circled above. Summing them,

$$P_e = (27 + 3\cdot 36 + 3\cdot 6 + 1)/2\cdot 343 = 78/343$$

With feedback, we may adopt the following strategy. For the first symbol, we will send an a_1 if $\underline{x}$ was selected, and an a_2 if $\underline{x}'$ was selected. As long as b_1's are received, we continue sending the same inputs. Whenever a b_2 is received, we switch the inputs.

$\Pr(\underline{y}/\underline{x})$	$\Pr(\underline{y}/\underline{x}')$
$\Pr(b_1b_1b_1/a_1a_1a_1) = 216/343$	$\Pr(b_1b_1b_1/a_2a_2a_2) = (27/343)$
$\Pr(b_1b_1b_2/a_1a_1a_1) = 36/343$	$\Pr(b_1b_1b_2/a_1a_1a_1) = (36/343)$
$\Pr(b_1b_2b_1/a_1a_1a_2) = (18/343)$	$\Pr(b_1b_2b_1/a_2a_2a_1) = 72/343$
$\Pr(b_2b_1b_1/a_1a_2a_2) = (9/343)$	$\Pr(b_2b_1b_1/a_2a_1a_1) = 144/343$
$\Pr(b_1b_2b_2/a_1a_1a_2) = 24/343$	$\Pr(b_1b_2b_2/a_2a_2a_1) = (12/343)$
$\Pr(b_2b_1b_2/a_1a_2a_2) = (12/343)$	$\Pr(b_2b_1b_2/a_2a_1a_1) = 24/343$
$\Pr(b_2b_2b_1/a_1a_2a_1) = 24/343$	$\Pr(b_2b_2b_1/a_2a_1a_2) = (12/343)$
$\Pr(b_2b_2b_2/a_1a_1a_1) = (4/343)$	$\Pr(b_2b_2b_2/a_1a_1a_1) = 16/343$

Summing, $P_e = (27 + 36 + 18 + 9 + 12 + 12 + 12 + 4)/2\cdot 343 = 65/343$

Exercise 3-4 Show that if $C_o^+ > 0$, $F(0) = F_\infty = F_{K-1}$

Solution:

Let $C_o^+ = -\ln \max_j \sum_{\substack{k \text{ for} \\ \text{which} \\ P_{j,k}>0}} P_k^* \geq -\ln [(K-1)/K]$

Let m_n be the number of words which the decoder perceives as possible messages after n digits have been received. At each stage of the transmission process, the transmitter divides these m_n words into K sets, the k^{th} set containing $P_k^* m_n$ words, as nearly as possible. We overbound m_n by $\bar{m}_n$, where

$$\bar{m}_o = M; \quad \bar{m}_{n+1} = \bar{m}_n \exp -C_o^+ + K-1$$

This is a valid upper bound because actually, if the j^{th} output symbol is received,

$$m_{n+1} = \sum_{\substack{k \text{ for which} \\ P_{j,k} > 0}} [m_n P_k^*]^{\pm} \leq m_n \sum_{\substack{k \text{ for which} \\ P_{j,k} > 0}} P_k^* + (K-1)$$

from which the upper bound follows by the definition of C_o^+. The solution of the recurrence for the upper bound is

$$\bar{m}_n = \bar{m}_\infty + (M - \bar{m}_\infty) \exp -nC_o^+$$

where $\bar{m}_\infty = (K-1)/(1-\exp -C_o^+) \leq (K-1)$

Select $N_1 = \ln M / C_o^+$, then $\bar{m}_{N_1} = \bar{m}_\infty + 1 - \bar{m}_\infty / M \leq K(K-1)$

These final K(K-1) words may be reduced to (K-1) words with less than K more questions, since if one or more words is placed on each input, at least one word may be discarded at each question. Hence,

$$F(R) \geq F_{K-1} (N-N_1)/N = F_{K-1}(1-R/C_o^+)$$

$$F(0) = F_{K-1}$$

Exercise 3-5:

Show that if $C_o > 0$, then $F(R) = \infty$ for $0 < R < C_o^+$, and $F(R) = E_{sp}(R)$ for $C_o^+ < R < C$.

Solution (Shannon, 1964)

For $R < C_o^+$, the solution follows directly from Exercise 3-4.

For $R > C_o^+$, we may define L by

$$L = - dE_{sp}(R)/dR$$

This L, introduced by Elias (1955), is equivalent to Gallager's ρ. According to theorems first proved by Elias and later extended by Gallager (1964), the exponent of the probability that the selected message does not appear among the top L+1 most probable words of a randomly chosen one-way code is given by $E_{sp}(R)$. So, given R and L, one may use random one-way coding with list decoding for the first N-log(L+1) digits. For the last log(L+1) digits, we may treat the channel with zero error capacity as a noiseless binary channel (by sending only two inputs that lead to no common outputs) and resolve any doubt the receiver may have about which of the (L+1) codewords was selected. Since L depends only on R (and not on N), the result follows as claimed.

Exercise 3-6

Consider a channel for which

Every input may reach A outputs ($A > 0$)
Every pair of inputs may reach B outputs ($B > 0$)
Every output is reachable from (K-I) inputs ($I > 0$)
All non-zero transition probabilities are given by p

Prove that, for such a channel, F(R) is a straight line. What are its endpoints?

Solution:

From Exercise 3-1, it is apparent that $C_o^+ = C = \ln pJ$. From Exercise 3.4, $F_\infty = F_{K-I}$, and F(R) is underbounded by the straight line between F_{K-I} and C_o^+. From the Shannon-Gallager theorem, F(R) is overbounded by this same straight line.

From Exercise 2-4, $F_{K-I} \geq E_{K-I} \geq E_K = E_2$. Thus, $F_{K-I} = F_2 = -\ln pB$.

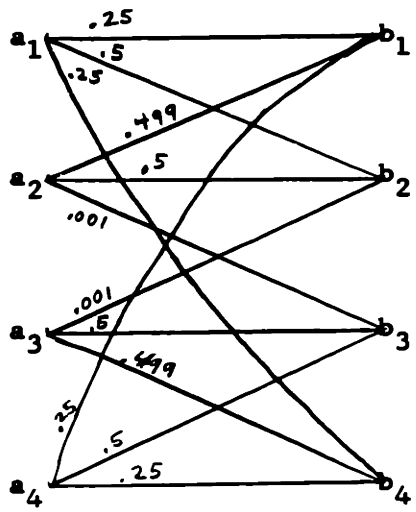
Exercise 3-7

Show by an example with K=4, I=1 that it is possible to have $C_o^+ > 0$ and $F_\infty < F_2$

Solution:

$C_o^+ > 0$

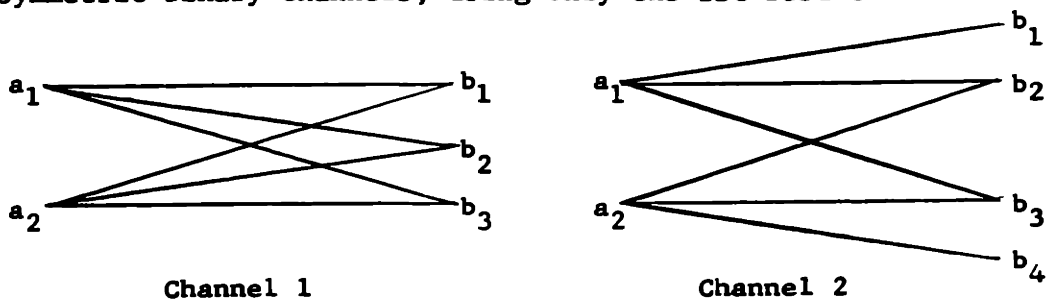
$F_\infty = F_3 < F_2$



Notice that $F_2 = -\ln(4 \cdot .001 \cdot .5)^{1/2}$ or about 1/2 ln 1000. However, we can see that F_3 is about 1/3 ln 1000, for given any triplet of inputs, they have a common output, which is reached from at least two of them with probability of the order of 1 and from at most one of them with a probability of the order of .001.

Exercise 3-8

Show that $F_\infty = -\ln \sum_j p_{j,1}^{1/3} p_{j,2}^{2/3}$ for the following symmetric binary channels, using only the BSC result.



Channel 1 Channel 2

Solution

For channel 1,

$P_e = \sum_{n=0}^{N} \binom{N}{n} p_{2,1}^n [(1-p_{2,1})P]^{N-n}$ where P is the probability of error per digit for a BSC with channel error probability of $p = p_{3,1}/(p_{1,1}+p_{3,1})$. For large block lengths, $P = (p^{1/3}q^{3/3} + p^{2/3} q^{1/3})$. Substituting this in the expression for P_e yields the claimed result.

For channel 2, let A denote the number of received b_1's and b_4's. Since we could ignore all such received symbols if we so chose,

$P_e \leq \binom{N}{A} p_{1,1}^A [(1-p_{1,1})P]^{N-A}$ where $P = (p^{1/3}q^{2/3} + p^{2/3}q^{1/3})$; $p = p_{3,1}/(p_{2,1} + p_{3,1})$. However, we do not ignore such received symbols. Whenever one is received, we may discard half of the words (since our order strategy has half the words on a_1 and half on a_2, within the nearest integer). If $A > 1 + \log M$, $P_e = 0$, so $\binom{N}{A}$ is only algebraic in N and the claim is true.

Chapter 4

ERROR CORRECTION CAPABILITY OF THE BINARY SYMMETRIC CHANNEL WITH FEEDBACK AT POSITIVE RATES

Chapter Abstract

After demonstrating the relationship between error exponent and error correcting capability, we evaluate the error correcting capabilities of various strategies for the binary symmetric channel with feedback. We first consider two simple-minded strate - gies: probability strategies and order strategies. We then derive general bounds on the error correction capability, and exhibit constructive procedures which asymptotically achieve these bounds over a large region of rates. The deficiencies of the simple-minded procedures are then exposed, and we conclude with comments on the problem of achieving asymptotically optimum error exponents.

Pages 48-53 of Chapter 3 are prerequisite to this chapter.

Distance, Error Correction Capability and Error Exponent

Ever since Hamming's (1950) pioneering paper on error correction codes, the concept of minimum distance has been widely used. It is defined as the minimum number of places in which any two codewords differ. Following the lead of Prange (1957), algebraists such as Bose-Chaudhuri(1960) and Mattson-Solomon(1961) have used this concept as a means of evaluating various codes which they have designed for one-way

binary symmetric channels and other Hamming metric channels.

A closely related concept is error correction capability, which we define as the maximum number of errors which the code is certain to correct. For one-way channels, the error correction capability, e, is the greatest integer less than half the minimum distance. The ultimate goal of coding is to minimize the error probability, not to maximize e, a point which the algebraists tend to overlook.† However, these two criteria are closely related, a point which the error exponent theorists sometimes overlook.

Many codes which have relatively poor error-correction capability actually have quite good exponents, because they succeed in correcting the overwhelming majority of error patterns which contain substantially more than e errors, even though there are a few patterns of only e errors which cause them to fail. Most random codes, for example, will have only a modestly good error-correction capability, yet they succeed in almost-certain error correction for any rate below capacity, as Shannon first proved in 1948. In the long run, the channel may be expected to make about Np errors. Any scheme which plans to utilize this channel by setting $e/N = p-\epsilon$, then correcting all patterns of e errors and no more, is inherently restricted to a rate far below capacity. It is possible, for example, to transmit information at a nonzero rate over a channel whose error probability is 49% ($C = 2.9 \times 10^{-4}$ bits/bit). Yet no code of any positive rate and sufficiently large block length can correct all error patterns even with $e/N = 25\%$, as has been demonstrated by Plotkin (1951). Roughly speaking, random codes will correct almost all error patterns of weight less than 2e,

† Led by A. M. Gleason, the algebraists have recently been devoting considerably more attention to errors beyond the minimum distance. Particularly noteworthy are contributions by MacWilliams (1963) and Pless (1963).

even when they fail to correct some error patterns of weight e.

In spite of all these contrary facts, there is actually a close relationship between the error-correcting capability and the error-exponent curves if the channel error probability is small. Since there is some uncorrectable error pattern of weight e + 1,

$$P_e \geq p^{e+1} q^{N-e-1} \tag{4.10}$$

Furthermore there are no fatal error patterns of weight e or less.

$$P_e \leq \sum_{k=e+1}^{N} \binom{N}{k} p^k q^{N-k} \tag{4.11}$$

The sum is dominated by the first term if $p/q < 1 - e/N$ (a quite reasonable assumption, since it is implied by $e/N < 1/4$ if $p \leq 3/7$, or by $e/N < 1/3$ if $p \leq 2/5$). So for large N these two bounds can be written as

$$-e/N \ln p - (1-e/N) \ln q \leq -1/N \ln P_e \leq -e/N \ln p - (1-e/N) \ln q + H(e/N) \tag{4.12}$$

For very noisy channels, in which both p and q are of the order to 1/2, the term H(e/N) is dominant and these bounds are worthless. In these cases minimum distance is not an important property. The behavior of the error-exponent vs rate curves in this and other very noisy situations has been studied by Reiffen (1963) and the asymptotic form of E(R) as p goes to 1/2 is known, thanks to the coincident lower and upper bounds given by Gallager (1964) and Shannon, Gallager, and Berlekamp (1965). (Some of the details are given in the last section of Chapter 2.)

We observe here that in the opposite limiting situation, as p goes to zero, the maximum error-correcting capability alone determines the exponent. From the above bounds, we see that

$$\lim_{p \to 0} \lim_{n \to \infty} -1/N \log P_e \to -e/N \log p \tag{4.13}$$

For infinitesmal channel error probability, the error exponent is the error-correction capability times -log p.

For channels without feedback, if the error-correction capability is e, then there is at least one code word at distance 2e+1. The probability of error is bounded by

$$P_e \geq 1/2 \binom{2e+1}{e} p^{e+1} q^e \tag{4.14}$$

because there are $\binom{2e+1}{e}$ ways of changing e+1 of the 2e+1 bits in which the two codewords differ. (It makes no difference whether any errors are made in the N-2e-1 bits in which the words agree.) Asymptotically,

$$-\ln P_e \leq -\ln (4pq)^e \tag{4.15}$$

At zero rate, the maximum error-correction capability was shown by Plotkin (1951) to be asymptotically N/4, which gives

$$E(0) \leq -1/4 \ln (4pq) \dagger \tag{4.16}$$

For channels with feedback, the term $\log 4^e$ can no longer be legitimately added to the error exponent. Minimum distance is no longer a well-defined concept, because there is no relation between the number of channel errors required to make the received word look exactly like some nontransmitted word and the number of errors required to make the transmitted word look more like this received word than

† From Chapter 2 it is apparent that this holds with equality.

any other. It is no longer true that there must be at least $\binom{2e+1}{e}$ ways of causing failure by making only e+1 channel errors. In general, no term of the type $\ln A^e$ ($A > 1$ and independent of p) can be added to the error exponent. As a proof, note that for sufficiently small p,

$$p^{1/3} q^{2/3} + p^{2/3} q^{1/3} < A^{1/3} p^{1/3} q^{2/3} \tag{4.17}$$

This contradicts a result of Chapter 3, which states that for the BSC,

$$F_\infty = -\ln (p^{1/3} q^{2/3} + p^{2/3} q^{1/3}) \tag{4.18}$$

For feedback channels, the minimum distance is evidently no longer a useful concept. Since there is no prescribed code word associated with each message, there is no relation between the number of errors necessary to make transmitted message $\underline{x}_1$ look exactly like transmitted message $\underline{x}_2$, the number of errors required to make $\underline{x}_1$ look more like $\underline{x}_2$ than like $\underline{x}_1$, and vice versa in both cases.

Equations (4.14) through (4.16) are invalid for channels with feedback. However, the maximum number of channel errors which can be certainly corrected is still well-defined as the error-correction capability, and equations (4.12) and (4.13) still apply directly to binary symmetric channels with feedback.

Thus the search for feedback strategies having maximum error-correction capability is justified. In addition to the interest it enjoys in its own right, the solution to this problem gives the limiting form of E(R) for very clean Hamming-metric channels.

Before proceeding to the investigation of general partitioning strategies, we derive a fundamental bound on the error-correcting capability using only three codewords

and we investigate the error-correcting capability of certain simple-minded strategies.

Error-Correction Capability Using Three Codewords

The error correction capability possible using only three codewords with feedback can be immediately deduced from certain results of Chapter 3. However, since we do not wish to require readers of this chapter to remember results of previous chapters (other than the first chapter), we give here an alternate derivation of this special case.

We assume Nature's role, take control of the channel, examine the users' feedback strategy, and maliciously select positions in which to place N/3 errors so as to lead the decoder astray. Our plot is to cause the received sequence to be such that two words end in a dead tie, and neither of them has more than N/3 votes against it. Whatever word the decoder selects might then be wrong even if no more than N/3 channel errors had occurred.

The method by which we cause two words each to accumulate less than N/3 unfavorable votes is as follows: As long as all three words are still in the running (i.e. none has accumulated more than N/3 negative votes) we answer the decoder's question in favor of whichever set contains 2(or 3) words, and against whichever set contains only 1 (or 0). Eventually one word might accumulate N/3 + 1 negative votes. It is then effectively out of the race, since the max-likelihood decoder will never decide in favor of it no matter what happens subsequently. When faced with the choice between the two words remaining, we answer in favor of the current underdog, and against the current leader. By this scheme, we prevent any answer from ever voting against more than 1 of the competitive words. Thus, after 3e +1 questions,

only one of the words can have received more than e negative votes. Conclusion: $n \geq 3e + 2$.

R. G. Gallager has suggested a slightly different plot by which Nature can also accomplish this same wicked end.

Probability Strategies

When one first considers the problem of selecting good partitions, he is likely to feel intuitively that the best strategies will partition the words into approximately equiprobable subsets. One would like the probability that either side of the partition fails to be as nearly equal to 1/2 as possible. We call any strategy which partitions the words in such a manner a probability strategy.

On the surface, probability strategies appear promising for several reasons. Only by probability strategies can the receiver obtain, on the average, the maximum amount of information about the selected message. Furthermore, Horstein (1963) has demonstrated certain sequential transmission procedures, using probability strategies, which give surprisingly large positive exponents at all rates less than and equal to capacity. Nevertheless, we shall show that for block coding, probability strategies have error correction capabilities which are markedly inferior to those of certain other strategies.

Let us assume that $M = 13$, and the channel probability is small, $p < 1/13$. Under these circumstances, $12p/q < 1$, so if one word has even a single-vote lead over the other 12, the probability strategy will play the top word against all the others:

$$\begin{matrix} 1 \\ 12 \end{matrix} = \begin{matrix} 1 \\ 0 \end{matrix} + \begin{matrix} 0 \\ 12 \end{matrix}$$

In general, the probability strategy will partition the words on the higher levels evenly, until it comes upon a level with an odd number of words. The words at that level will be partitioned as evenly as possible, and all lower words will be placed together against the side which got the larger half. Specifically, each of the following situations will be partitioned as shown:

$$13 = 7 + 6 \; ; \qquad \begin{matrix} 7 \\ 6 \end{matrix} = \begin{matrix} 3 \\ 6 \end{matrix} + \begin{matrix} 4 \\ 0 \end{matrix} \; ; \qquad \begin{matrix} 3 \\ 10 \end{matrix} = \begin{matrix} 1 \\ 10 \end{matrix} + \begin{matrix} 2 \\ 0 \end{matrix}$$

If the channel behaves in a particular manner, the following sequence of states will occur:

$$13 \quad \begin{matrix} 7 \\ 6 \end{matrix} \quad \begin{matrix} 3 \\ 10 \end{matrix} \quad \begin{matrix} 1 \\ 12 \end{matrix} \quad 13$$

It is possible for this cycle to recur again and again. During each four questions, each word accumulates only one additional negative vote. During N questions, each word accumulates only N/4 negative votes. We conclude that the error correction capability of any probability strategy is at most N/4, if $M \geq 13$, and $p < 1/13$.

We know that at zero rate it is possible to correct up to N/3 errors using order strategies.† It is apparent that, under the circumstances mentioned above, probability strategies have error-correction capabilities which are inferior to the error-correction capabilities of order strategies. From the result of the previous section, it follows that the error exponents for probability strategies are likewise inferior, for sufficiently clean binary symmetric channels. In particular, for probability strategies on channels with $p < 1/13$,

$$F_{13} \leq -\ln p^{1/4} q^{3/4} < -\ln (p^{1/3} q^{2/3} + p^{2/3} q^{1/3})$$

† For proof, apply (4.13) to F_∞

Order Strategies†

As in Chapter 3, we now consider order strategies. An order strategy is one which always partitions the words into two sets which depend only on the ranks of the various words, and not on the relative differences in the number of votes against them. For example, consider the order strategy that plays the 1st, 3rd, 5th, 7th, ... most probable words against the 2nd, 4th, 6th, 8th, ... most probable words. Figuratively,

1
2
3
4
5
6
7
...
...

This order strategy fulfills our desire to bisect the words above any given level as nearly as possible. It happens that this order strategy is exponentially optimum at zero rate, as we mentioned in Chapter 3. In this section we will investigate the error-correction capability of this strategy at positive rates.

Let $w_j(n)$ denote the number of words with j votes against them after n questions have been asked. Then, except for Diophantine constraints,

$$w_j(n+1) = 1/2\ (w_j(n) + w_{j-1}(n)\ )$$

and initially,

$$w_o(0) = 2^k$$

† Readers unfamiliar with Chapter 3 should omit this section and skip to p. 120, after looking at Figures 4-4 and 4-5 on p. 118 and 119.

The solution of this recurrence is

$$w_j(n) = 2^{k-n} \binom{n}{j}$$

which may be verified directly. Let j' be the number of votes against the L^{th} word. Approximately, $j' \approx j$, where j is given implicitly by

$$L = \sum_{m=0}^{j} w_m = 2^{k-n} \sum_{m=0}^{j} \binom{n}{m}$$

Asymptotically,

$$\ln L = k - n + nH(j/n)$$

If $\ln L << n$, then the left hand side may be ignored, giving

$$H(j/n) = 1 - k/n$$

For fixed k, this gives a relationship between j and n as the game progress. A plot of this relationship is given in Fig. 4-1.

We next observe that the Diophantine constraints we so blithely neglected are, in fact, of no asymptotic consequence. To see this we note that, at each question, we can obtain an inequality comparing j', the actual number of votes against the L^{th} word with the j defined above. To get the bound in one direction, we remove the topmost word from the game after each question which favored it. By ignoring that word, we assure that at least half of the words above the L^{th} word have fallen. To get the bound in the other direction, we insert a new word on top of the pack after each question which did not favor the top word. Counting the new word, at most half of the words above the L^{th} word have just fallen. Due to the added or deleted words, after n questions the word that is actually in the L^{th} position may now appear as high as the $(L-n)^{th}$ position or as low as the $(L+n)^{th}$. Thus, the actual position of the L^{th} word

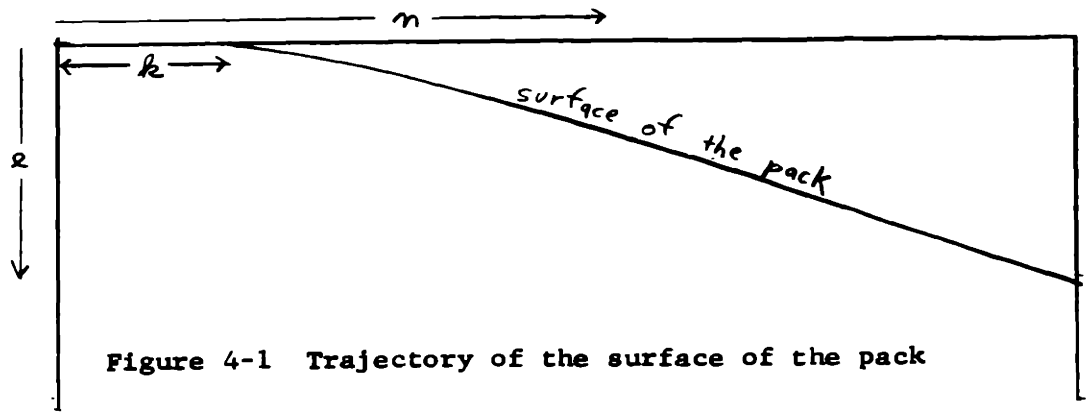


Figure 4-1 Trajectory of the surface of the pack

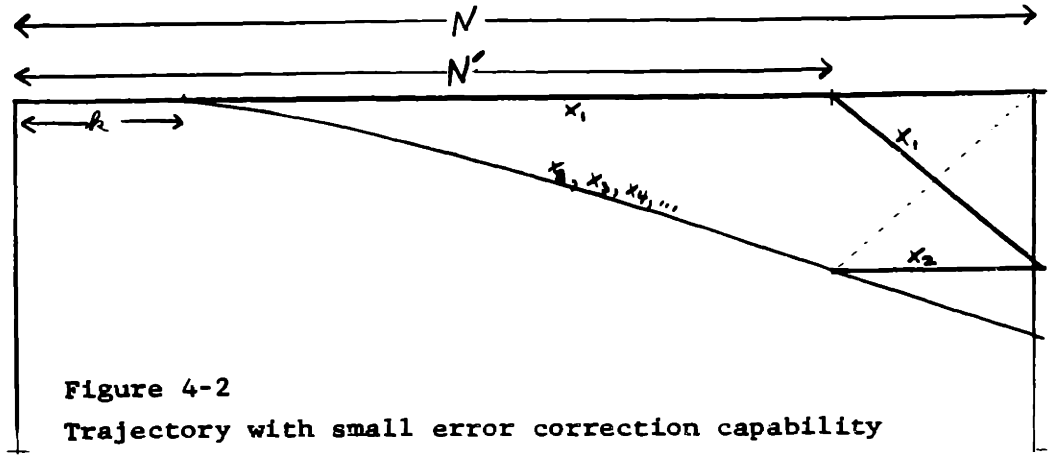


Figure 4-2
Trajectory with small error correction capability

is bounded by

$$j_o \leq j' \leq j_1,$$

where

$$L\text{-}n = \sum_{m=0}^{j_o} w_m \quad ; \quad L\text{+}n = \sum_{m=0}^{j_1} w_m$$

Since $\ln n << n$, the asymptotic relation

$H(j'/n) = 1 - k/N$ is still valid if $\ln L << n$.

This equation, as plotted in Fig. 4-1, defines the trajectory of the top of the pack. Immediately beneath this trajectory there must be a great number of words. Above this trajectory, however, there are very few words. It is possible that there are no words at all above the pack. Certainly there must be less than n words above the pack. Further considerations show that actually there must be far fewer than n words there, because all of the words there are being played against each other at every question. Even if there are only two words above the pack, they cannot remain there indefinitely, for their average must fall by 1/2 at every question. The top of the pack always falls more slowly, so eventually we can expect the second word to sink back into the pack. It may happen, of course, that this may be hindered by crossunders with the third word, which is also above the pack, but this cannot persist indefinitely either. In general, we expect only a small number of sparsely spaced words above the pack.

Since the first and second words must fight each other unmercifully as long as both are above the pack, the most probable single error pattern (i.e., the pattern which limits the error correction capability) results when the second word remains on the surface of the pack until quite near the end of the game. For the first N′ questions,

the top word receives no negative votes whatsoever. During these N' questions the second word stays on the surface of the pack, accumulating e negative votes, where e is given by

$$H(e/N') = 1 - k/N'$$

Then the final e questions all favor the second word. During these final e questions, the first word drops by e votes and ends the block tied with the second word. This trajectory is plotted in Fig. 4-2. The total block length is given by $N = N' + e$ or $N/N' = 1 + e/N'$. The relationship between the fractional error-correction capability, e/N and the rate $R = k/N$, may be readily determined graphically. Let R', $(e/N)'$, be a point on the Hamming volume bound curve of Fig. 4-3. The point $R = R'/(1+(e/N)')$, $e/N = (e/N)'/(1 + (e/N)')$, then lies on the error correction capability curve for the order strategy. This curve is plotted in Fig. 4-3 at the end of this section.

It can also be shown that other order strategies do just as poorly, or worse.

Figure 4-3

ERROR CORRECTION CAPABILITY OF THE BINARY SYMMETRIC CHANNEL WITH FEEDBACK USING ORDER STRATEGIES

NOTE:

$$\frac{\mathcal{E}}{N} = \lim_{p \to 0} \frac{\lim_{N \to \infty} -1/N \ln P_e}{-\ln p}$$

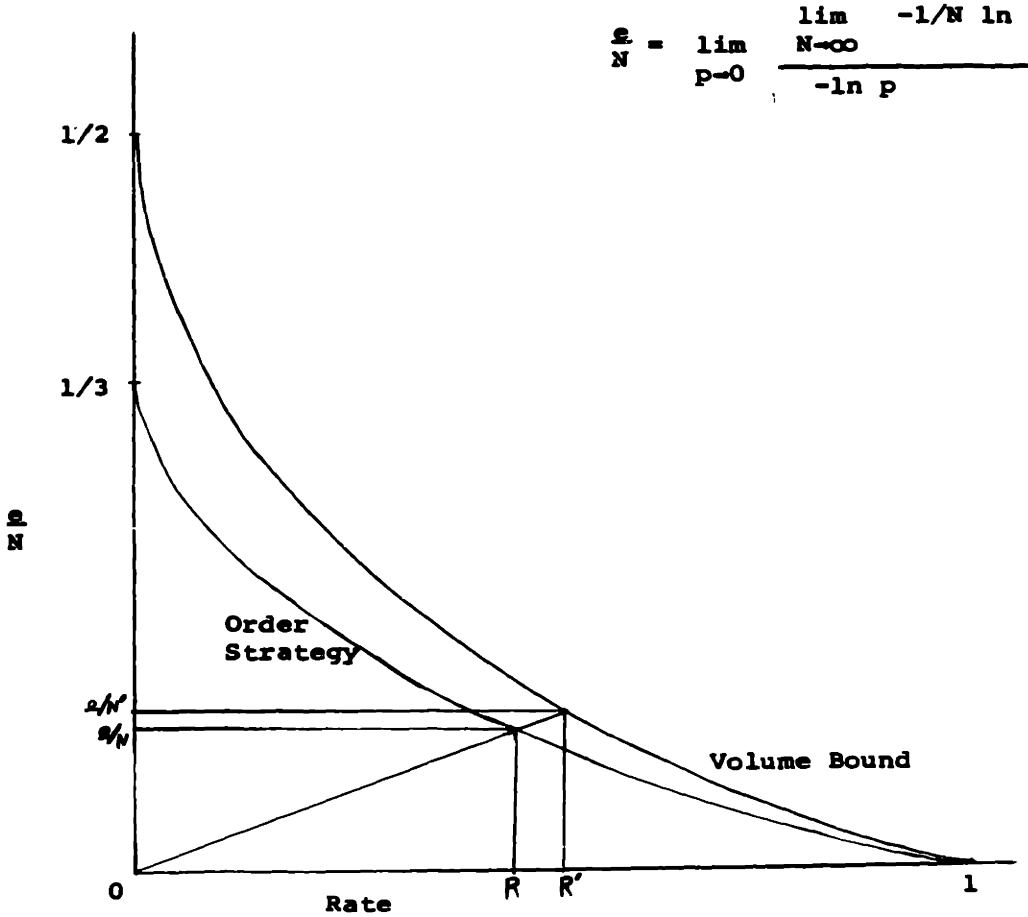


Figure 4-4

ERROR CORRECTION CAPABILITY OF THE BINARY SYMMETRIC CHANNEL WITHOUT FEEDBACK

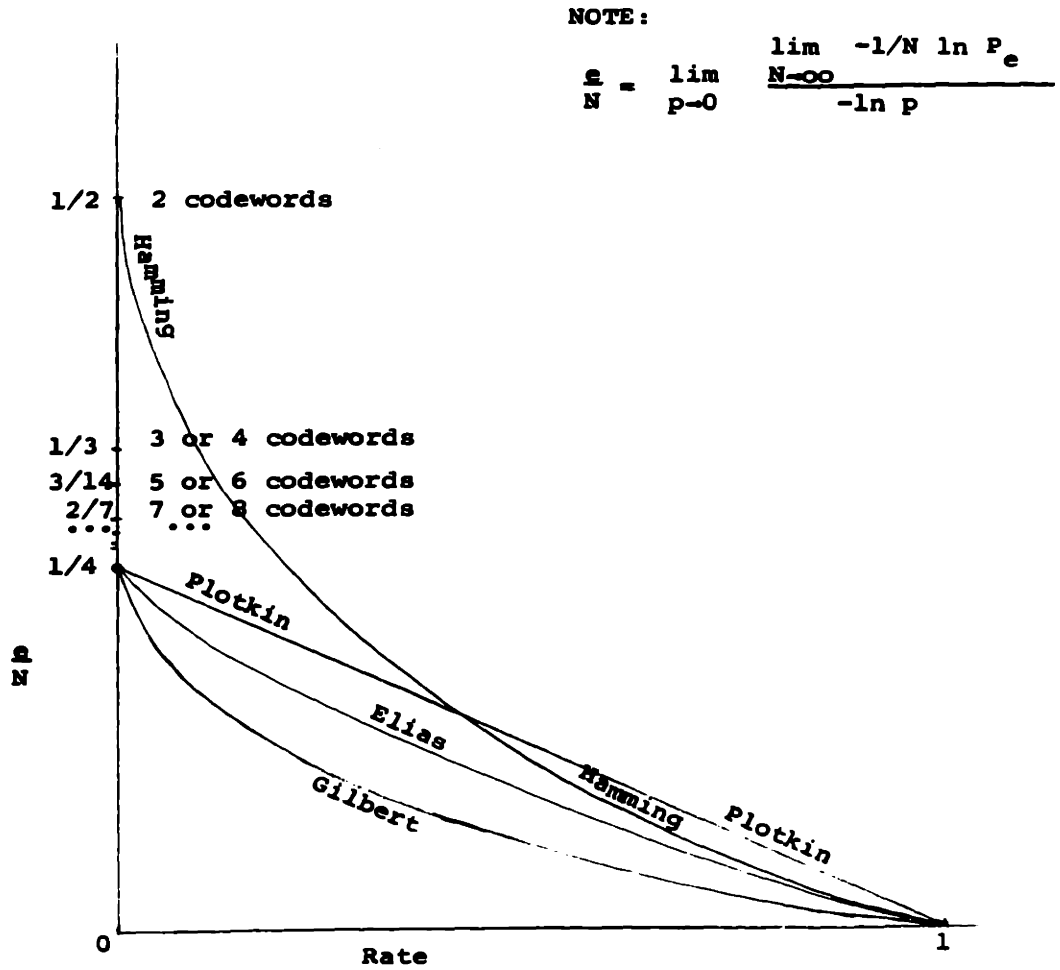
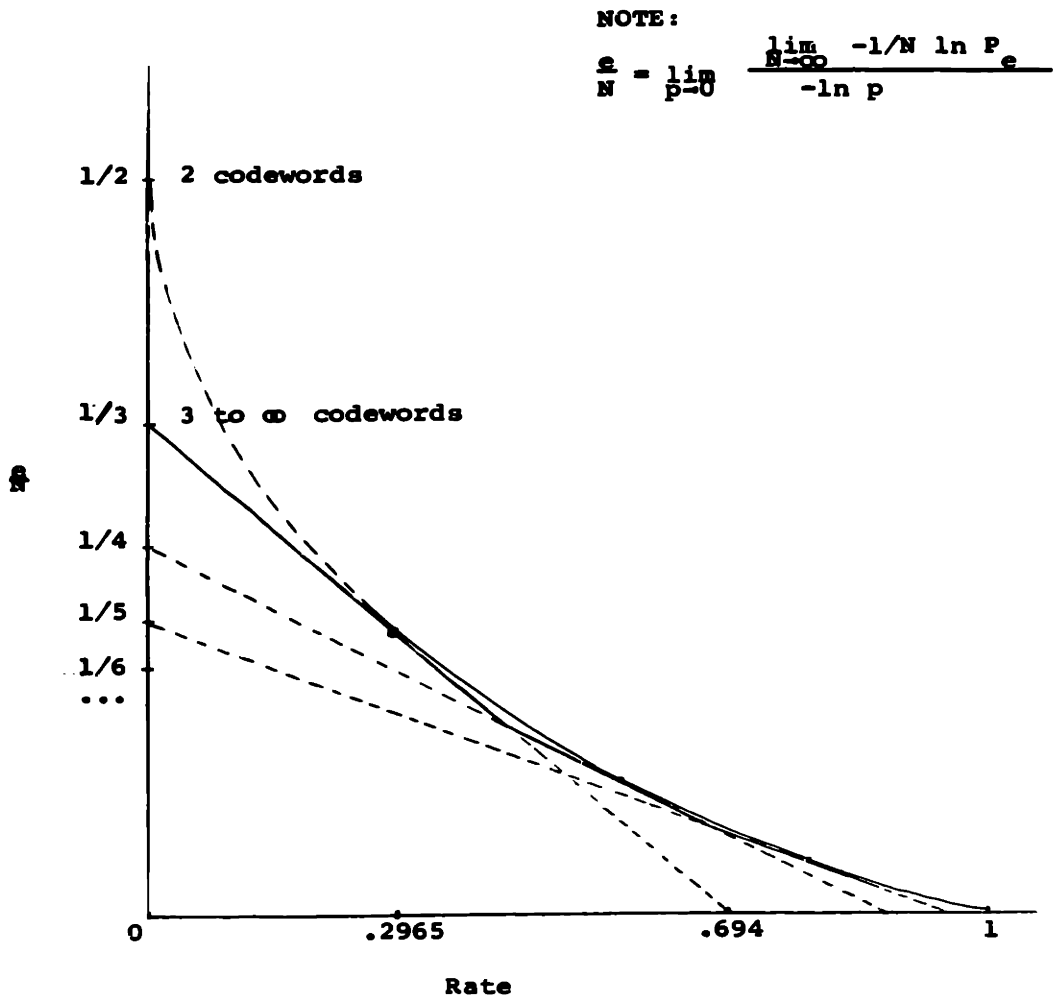


Figure 4-5

ERROR-CORRECTION CAPABILITY OF THE BINARY SYMMETRIC CHANNEL WITH FEEDBACK



GENERAL STRATEGIES WHICH CORRECT ALL PATTERNS OF e ERRORS

We now turn our attention to the problem of selecting a questioning strategy which guarantees that after all N questions have been asked, the receiver will be able to deduce correctly which word was transmitted unless the channel has made more than e errors. As before, after each question we tally the number of negative votes against each code word. However, we may now throw some of the words away before the end of the game. Since the number of channel errors is $\leq e$, words which accumulate more than e unfavorable votes may be disqualified from further consideration.

After each question, we record the number of words which have 0 negative votes, the number which have 1 negative vote, ... the number which have e negative votes. We write these numbers as components of a column vector, and call this vector the state of the game. If there are n questions remaining, this vector is called an n-state. The topmost components of this vector are often zeros. For this reason, we index the components from the bottom up and omit any zeros above the highest nonzero component:

$$\begin{matrix} \cdots \\ c_4 \\ c_3 \\ c_2 \\ c_1 \\ c_0 \end{matrix} = \underline{c}$$

The component c_i denotes the number of words which have received e-i negative votes.

The receiver partitions the present state of the game into two substates, and asks the source which substate contains the message. The (noisy) answer constitutes

a vote against one substate or the other. The next state of the game is then a new list of numbers of words having received various numbers of negative votes. The general situation is depicted below:

n-state	partition	resulting(n-1)-state if answer favors left	resulting(n-1)-state if answer favors right
c_4	a_4 b_4	a_4	b_4
c_3	a_3 b_3	$a_3 + b_4$	$a_4 + b_3$
c_2	a_2 b_2	$a_2 + b_3$	$a_3 + b_2$
c_1	a_1 b_1	$a_1 + b_2$	$a_2 + b_1$
c_0	a_0 b_0	$a_0 + b_1$	$a_1 + b_0$
	$a_i + b_i = c_i$	$c'_i = a_i + b_{i+1}$	$c'_i = a_{i+1} + b_i$

It is frequently more convenient to discuss only the current state and the pair of states which may result from it, without being too concerned about the details of the partition which brings this about. This nonchalantness is justified by the following theorem:

Partitioning Theorem: There exists a partition which reduces the state $\underline{x}$ into the states $\underline{y}$ and $\underline{z}$ iff

1) $\underline{x} \geq 0$; $\underline{y} \geq 0$; $\underline{z} \geq 0$ (all components are nonnegative)

2) $x_{i+1} + x_i = y_i + z_i$ for all i, $0 \leq i \leq e$

3) For all I, $0 \leq i \leq e$

$$\sum_{i=I}^{e} y_{2i+2} \leq \sum_{i=I}^{e} z_{2i+1} \leq \sum_{i=I}^{e} y_{2i}$$

and

$$\sum_{i=I}^{e} z_{2i+2} \leq \sum_{i+I}^{e} y_{2i+1} \leq \sum_{i=I}^{e} z_{2i}$$

For given $\underline{x}$, $\underline{y}$, and $\underline{z}$, this partition is unique.

Proof: Without 1), the vectors $\underline{x}$, $\underline{y}$, and $\underline{z}$ are not really states and partitioning is meaningless. Among nonnegative vectors, a partition exists iff there are two substates $\underline{u}$ and $\underline{v}$ such that

$$\underline{x} = \underline{u} + \underline{v}$$

$$y_i = u_i + v_{i+1} \; ; \; z_i = v_i + u_{i+1} \qquad \text{for all } i.$$

We will show that given $\underline{y}$ and $\underline{z}$, both $\underline{x}$ and the unique partition can be determined subject to conditions 2) and 3). Solving for $\underline{x}$ is most readily accomplished by computing the highest components first and working down.

$$x_e = u_e + v_e = y_e + z_e$$

In general, $x_i + x_{i+1} = u_i + u_{i+1} + v_i + v_{i+1} = y_i + z_i$, and thus $\underline{x}$ can be computed from the topmost component working down, using the equation $x_i = y_i + z_i - x_{i+1}$.

We may also solve for $\underline{u}$ and $\underline{v}$ in terms of $\underline{y}$ and $\underline{z}$

$$\sum_{i=I}^{e} y_{2i+1} = \sum_{i=I}^{e} (u_{2i+1}) + v_{2i+2}) \; ; \quad \sum_{i=I}^{e} z_{2i} = \sum_{i=I}^{e} (v_{2i} + u_{2i+1})$$

$$v_{2I} = \sum_{i=I}^{e} (v_{2i} - v_{2i+2}) = \sum_{i=I}^{e} (z_{2i} - y_{2i+1})$$

Similar expressions are found for the odd components of $\underline{v}$, and for the odd and even components of $\underline{u}$. Condition 3) is the statement that these components be nonnegative. Q. E. D.

For some n-states, it is possible to devise a partitioning strategy for the remaining n questions which ensures that all words but one will eventually receive

more than e negative votes; for other n-states no such strategy exists. We call the former winning n-states; the latter, losing n-states. A 0-state is winning iff only one word has e or less negative votes. These considerations justify the following definitions:

A 0-state $\underline{x}$ is winning iff $\Sigma x_i \leq 1$. A nonzero winning 0-state is called a singlet. An n-state is winning iff it can be reduced to two winning (n-1)-states. (The two winning (n-1)-states need not be distinct.)

Several lemmas follow at once:

Lemma 1: Any vector which is a winning n-state is also a winning j-state, for any $j > n$. Singlet states are winning n-states for all n.

Any vector which is a winning j-state but a losing (j-1)-state is said to be a borderline winning j-state.

Lemma 2: The only borderline winning 1-state is $\begin{matrix} 0 \\ \cdots \\ 0 \\ 2 \end{matrix}$.

Omitting top zeros, this state is written as 2.

If $\Sigma x_i = 2$, $\underline{x}$ is called a doublet. The winning partition of any doublet plays the two words against each other. This consideration leads to the following result:

Lemma 3: A doublet $\underline{c}$ is a winning n-state iff $\Sigma i c_i \leq n-1$, with equality in the borderline case.

Lemma 4: If $\underline{c} \leq \underline{d}$ (meaning $c_i \leq d_i$ for all i) and $\underline{d}$ is a winning n-state, then $\underline{c}$ is also a winning n-state.

The conclusion of Lemma 4 is also valid under slightly weaker hypotheses:

Lemma 4′: If $\sum_{i=k}^{e} c_i \leq \sum_{i=k}^{e} d_i$ for all k, and $\underline{d}$ is a winning n-state, then $\underline{c}$ is also a winning n-state.

Lemma 5: M is a winning n-state iff $M \leq 2^n$. The best partition of the state M is one which plays half the words against the other half.

Figure 4-6

SOME WINNING n-STATES, $1 \leq n \leq 9$

i	n:	9	8	7	6	5	4	3	2	1
0		512	256	128	64	32	16	8	4	2
1		50	28	16	8	4	2	2	1	
0		12	4	0	8	8	6	0	1	
2		1	1	1	1	1	1	1		
1		0	0	0	0	0	0	0		
0		456	219	99	42	16	5	1		
2		1	1	1	1	1	1			
1		43	22	11	4	1	1			
0		36	21	11	14	10	0			
.		.	2	2	2	2				
.		.	0	0	0	0				
.		.	182	70	20	0				
		.	2	2						
		.	20	6						
		.	2	22						
		7	3							
		0	0							
		190	145							
		7	3							
		15	14							
		40	19							
		8	4							
		0	0							
		144	108							
		8	4							
		8	8							
		64	36							
		1	1	1	1	1	1			
		4	1	1	0	0	0			
		14	10	0	1	1	0			
		58	36	35	15	0	1			
		.	.	1	1	1				
		.	.	0	0	0				
				5	0	0				
				24	22	6				

A table of some of the winning n-states, for $1 \leq n \leq 9$ is given in Fig. 4-6.

An examination of this table leads us to some deeper results. Foremost among these is a volume bound, which is a generalization of Hamming's (1950) bound for one-way codes. The primary difference is that our bound surrounds words at different levels with different sizes of spheres.

The appropriate definition of the volume of an n-state $\underline{x}$ is obtained by surrounding all words at height j by a sphere of radius j:

$$V_n(x) = \sum_{i=0}^{e} x_i \sum_{j=0}^{i} \binom{n}{j}$$

Theorem (Conservation of Volume): Let $\underline{x}$ be any nontrivial n-state, and let $\underline{y}$ and $\underline{z}$ be the (n-1)-states which result from it following any given partition. Then $V_n(\underline{x}) = V_{n-1}(\underline{y}) + V_{n-1}(\underline{z})$.

Proof: Let $\underline{x} = \underline{u} + \underline{v}$ be the partition which reduces $\underline{x}$ to $\underline{y}$ and $\underline{z}$. Then the theorem becomes

$$\sum_{i=0}^{e} (u_i + v_i) \sum_{j=0}^{e} \binom{n}{j} = \sum_{i=0}^{e} (u_i + v_i + u_{i+1} + v_{i+1}) \sum_{j=0}^{i} \binom{n-1}{j}$$

Since x_i is arbitrary, an equivalent theorem is

$$\sum_{j=0}^{i} \binom{n}{j} = \sum_{j=0}^{i} \binom{n-1}{j} + \sum_{j=0}^{i} \binom{n-1}{j}$$

This is true, because by expanding both sides into factorials one readily verifies that

$$\binom{n}{j} = \binom{n-1}{j} + \binom{n-1}{j-1} \qquad \text{Q.E.D.}$$

One immediate application of this result is the following

Volume Bound Theorem: If $\underline{x}$ is a winning n-state, then $V_n(\underline{x}) \leq 2^n$.

Proof: The theorem is true for n=0, for in fact a singlet state satisfies any volume bound:

$$\sum_{k=0}^{\infty} \binom{j}{k} = \sum_{k=0}^{j} \binom{j}{k} = 2^j$$

For arbitrary n, the theorem follows directly from the conservation of volume theorem by induction. Q. E. D.

In some special cases this bound is the only requirement. Lemma 5 showed one such case. Doublet states are another, as is shown by the following restatement of Lemma 3:

Lemma 3′: A doublet state $\underline{c}$ is a winning n-state iff $V_n(\underline{c}) \leq 2^n$. Equality occurs in the borderline case.

Proof: Let the only nonzero components of $\underline{c}$ be $c_i = 1 = c_j$ (where possibly i = j). Then the borderline case of Lemma 3 becomes i + j = n-1. In this case

$$V_n(\underline{c}) = \sum_{k=0}^{i} \binom{n}{k} + \sum_{k=0}^{j} \binom{n}{k} = \sum_{k=0}^{i} \binom{n}{k} + \sum_{k=n-j}^{n} \binom{n}{n-k} = \sum_{k=0}^{n} \binom{n}{k} = 2^n \quad \text{Q. E. D.}$$

Lemma 3′ has shown that for doublets, the volume bound is the only restriction that must be satisfied. In general, however, there are losing states which still satisfy the volume bound. For example, consider the 4-state $\begin{matrix}3\\0\end{matrix}$. It's volume is $3(\binom{4}{0} + \binom{4}{1}) = 15 < 16 = 2^4$, but this is nevertheless a losing state. We proved earlier that $n \geq 3e + 2$; this precludes the possibility of a winning 4-state with e = 1. A generalized version of this limitation is the following

Translation Bound Theorem: If $\Sigma x_i \geq 3$, then $\underline{x}$ cannot be a winning n-state unless $T\underline{x}$ is a winning (n-3)-state. $T\underline{x}$ is the translation of $\underline{x}$, defined by $(T\underline{x})_i = x_{i+1}$.

Proof: The basic idea is again an induction on n. We first verify by exhaustion that the theorem is true for small n. Figure 4-6, page 125. Now suppose that the theorem is true for $n \leq k-1$, and that $\underline{x}$ is a winning k-state. There must then exist some partition of $\underline{x}$ which reduces it to $\underline{y}$ and $\underline{z}$, which are winning (k-1)-states. When this same partition is applied to $T\underline{x}$, it reduces $T\underline{x}$ to $T\underline{y}$ and $T\underline{z}$. If $\Sigma y_i \geq 3$ and $\Sigma z_i \geq 3$, then the induction hypothesis guarantees that $T\underline{y}$ and $T\underline{z}$ are both winning (k-4)-states. Thus, $T\underline{x}$ is a winning (k-3)-state.

In the exceptional case that $\Sigma y_i \leq 2$, we must resort to special considerations. The translation bound, as stated, does not apply to such states. In fact, from Lemma 3, if the doublet $\underline{y}$ is a borderline winning n-state, then $T\underline{y}$ is a borderline winning (n-2)-state. If $\underline{y}$ is not a borderline (k-1)-state, then $T\underline{y}$ is a winning (k-3) state. Thus only the borderline doublet must be considered.

Define $\underline{x}'$ by $x'_o = 0$; $x'_k = x_k$ for all $k > 0$. Then $\underline{x}' \leq \underline{x}$ and $V_n(\underline{x}') \leq V_n(\underline{x})$. Since $\underline{y}$ is a reduction from $\underline{x}$, $\sum_{i=0}^{e} y_i \geq \sum_{i=1}^{e} x_i = \sum_{i=0}^{e} x'_i$. Thus $\underline{x}'$ is a singlet or a doublet. If it is a singlet, so is $T\underline{x} = T\underline{x}'$, and the proof is completed. If $\underline{x}'$ is a doublet, there are two possibilities. Either $\underline{x}' = \underline{y}$, or $\underline{x}'$ is a borderline winning k-state (because the doublet $\underline{x}$ reduces to $\underline{y}$ and $\underline{y}$ is a borderline winning (k-1)-state). If $\underline{x}' = \underline{y}$ then $T\underline{x} = T\underline{y}$ and $T\underline{x}$ is a winning (k-3)-state (because it is a translate of the winning doublet (k-1)-state).

If instead, $\underline{x}'$ is a borderline winning k-state, then it satisfies the volume bound with equality: $V_k(\underline{x}') = 2^k$. But $\underline{x}$ is also a winning k-state. $\underline{x} = \underline{x}'$ is the only possibility. In this case $T\underline{x}$ is not a winning (k-3)-state, but $\underline{x}$ is a doublet, so this case lies outside the hypotheses of the theorem.

Having verified the theorem in all the exceptional cases, we have completed

the proof. Q.E.D.

Together, the volume bound and the translation bound immediately eliminate most of the losing states. They are not exhaustive, however, for there are a few losing states which satisfy both bounds. For example, $\binom{51}{2}$ is a losing 9-state, even though it satisfies the volume bound and 51 is a winning 6-state. In spite of such isolated cases, however, we shall find that in the asymptotic cases of interest, these two bounds are all inclusive.

The volume and translation bounds apply to all possible n-states. The special n-states of greatest interest are ones in which the initial state $\underline{I}$ contains only one nonzero component: $I_e = M = 2^k$. We wish to find the minimum N for which $\underline{I}$ is a winning N-state. The information rate is then defined by R = k/N; the allowable error fraction is denoted by f = e/N. For small values of N, the possible values of R and f can be derived from our table. We note, for example, the occurrence of $\binom{16}{0}$ among our list of winning 7-states. (There is actually a one-way partitioning strategy which accomplishes this win, called the Hamming (7, 4) single-error-correcting code. (Hamming, 1950).) For N > 9, however, the detailed extension of the table involves considerable labor and we must rely instead on asymptotic bounds which we shall now derive. We are interested in the cases when N grows very large while f and R remain fixed.

The Volume Bound and Its Tangents

Recall f = e/N. We first consider the volume bound: $2^k \sum_{j=0}^{e} \binom{N}{j} \leq 2^N$.

Asymptotically this becomes $H(f) \leq 1-R$, or $R \leq 1-H(f)$. This is identical to Hamming's bound for one-way codes. A plot of the bound is found in Figs. 4-3, 4-4 and 4-5 at the beginning of this section, (pages 117-119).

Because of their frequent occurrence in the subsequent sections, the tangents to this curve are quite important. We digress here briefly to derive the equations for these tangent lines.

Consider a straight line which intercepts the f axis at f_o, the R axis at R_o, and which is tangent to the curve R / 1-H(f) at the point $R = R_t$, $f = f_t$. Define g = 1-f. Then the equations giving the point of tangency are

$$R(f_t) = 1-H(f_t) = R_o(1-f_t/f_o)$$

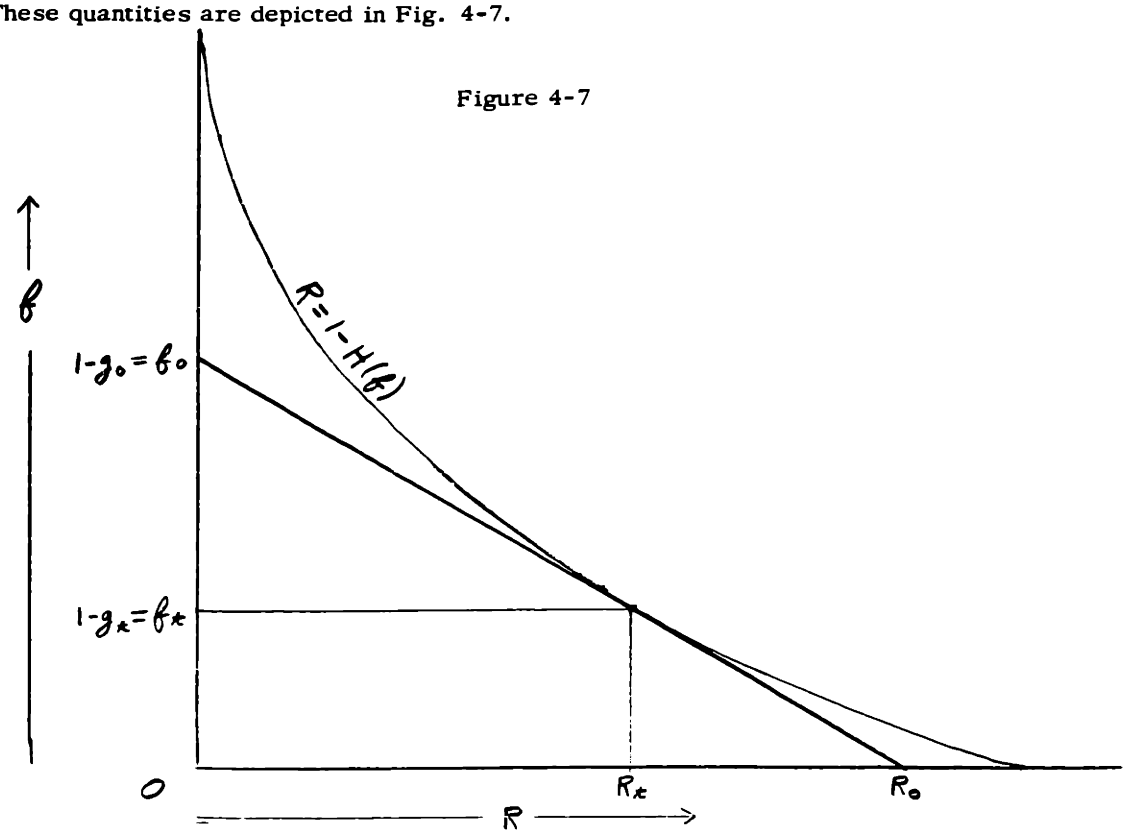
$$R'(f_t) = \log (f_t/g_t) = -R_o/f_o$$

and

$$f_t + g_t = 1.$$

These quantities are depicted in Fig. 4-7.

Figure 4-7



Subtracting f_t times the second equation from the first equation gives

$$R_o = 1 + \log g_t$$

Substituting this expression into the second equation and exponentiating gives

$$2^{f_o} f_t^{g_o} g_t^{} = 1$$

Introducing the quantity

$$s = g_t/f_t;\ \log s = R_o/f_o;\ f_t = 1/(1+s);\ R_t = (f_o - 1/(1+s)) \log s$$

permits the problem to be transformed into an equation in only one unknown:

$$1 = 2^{f_o} f_t^{g_o} g_t = 2 f_t^{g_o} s^{g_o} = 2s^{g_o}/(1+s)$$

or

$$2s^{g_o} = 1+s \ .$$

In the special case in which g_o is a rational number, this equation is algebraic. $s = 1$ is always an extraneous root of this equation; it may be removed by dividing through by $s-1$. The computation of the coordinates of the tangency point then reduces to the solution of this final algebraic equation.

Example:

$g_o = 2/3$. In this case the equation is

$$2s^{2/3} = 1+s$$

$$8s^2 = s^3 + 3s^2 + 3s + 1$$

$$0 = s^3 - 5s^2 + 3s + 1 = (s-1)(s^2 - 4s - 1)$$

$$s = 2 + 5^{1/2} = ((1+5^{1/2})/2)^3$$

$$f_t = (3 + 5^{1/2})^{-1} = .19095$$

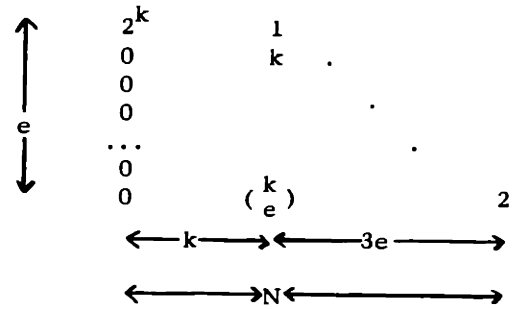
$$R_t = (1/3 - 1/(3 + 5^{1/2})) \log(2 + 5^{1/2}) = .29650$$

$$R_o = \log ((1 + 5^{1/2})/2) = .69425$$

A Plotkin-like bound

More bounds on f and R for large N may be obtained by combining the translation bound with the volume bound in various ways. Since $2^k \geq 3$ in the asymptotic case of interest, we conclude at once that $f \leq 1/3$.

The most obvious improvement of this bound may be obtained by examining a typical sequence of n-states that might occur as the questioning progresses:



The original N-state $\underline{I}$ has all 2^k words at level e. The first k questions can do no better than to bisect each component at each partition. After k questions, the (N-k)-state has a j^{th} component whose value is $\binom{N}{e-j}$. The second component from the top is $k > 3$, and hence at least 3e more questions are needed to bring this down. The conclusion is that $N \geq k + 3e$, or $R \leq 1-3f$.

The weakness of this direct approach is that actually a good many questions may be needed after the first k questions before the resulting state is sparse enough to be finished off with only 3e more questions. Attempts to measure this excess fail, but a

more devious attack does result in the desired bound:

The Tangential Bound

The best possible asymptotic bound is obtained by the following argument:

We first apply the translation theorem: If the initial state $\underline{I}$ (which has 2^k words at height e) is a winning N-state, then $T^m \underline{I}$ must be a winning (N-3m)-state, for any $0 < m < N/3$. Applying the volume bound to this state gives

$$2^k \binom{N-3m}{e-m} \leq 2^{N-3m}$$

Define $x = N-3e$; $y = e-m$. The bound becomes

$$8^{-y} \binom{x+3y}{y} \leq 2^{x-k}$$

The validity of this bound is restricted only by the requirement that $0 < y < e$, and it behooves us to choose the best y to obtain the strongest bound. This is accomplished by maximizing the left size of the above inequality. This can be done most readily by setting equal to one the ratio of the value of this expression for y to its value for y+1. For large y, this gives

$$1 = \frac{(x+3y)^3}{8\, y(x+2y)^2}$$

$$0 = (x+y)\,(x^2 - 5y^2)$$

$$y = 5^{-1/2}\, x$$

Plugging this value into the bound, and taking logarithms gives

$$x(1+3 \cdot 5^{-1/2})\, H(1/(3+5^{1/2})) \leq x(1+3 \cdot 5^{1/2}) - k$$

or

$$R(1+3 \cdot 5^{-1/2}) \leq (1-3p)\,(1-H(1/(3+5^{1/2}))\,)$$

The result is valid in the region $0 < y < e$, which is equivalent to the requirement that

$$(3+5^{1/2})^{-1} < f < 1/3$$

Comparing these numbers with the computed tangents to the volume bound, we see that this bound is a straight line which goes from the point $R = 0$, $f = 1/3$ to the volume bound, where it comes in tangentially and then ends. A plot of this bound is given in Fig. 4-4, page 119.

The form of this bound is quite analagous to a general one-way bound which Shannon and Gallager have recently derived for error exponents. For infinitesmal channel error probability, this bound coincides theirs.

In the next section we shall show that this bound is actually attainable.

SEQUENCES OF WINNING STATES

Having completed proofs of the volume bound, the translation bound, and their asymptotic combination, we are naturally led to investigate the possibility of finding specific winning states which lie on or close to these bounds. We start by an examination of our table of winning states for small n, (Figure 4-7). We know that in order to find any substantial (≥ 3) number of words at the top component, we are restricted to states for which $n \geq 3e + 2$. Thus if $e = 0$, $n \geq 2$, and we find that 4 is indeed a winning 3-state. If $e = 1$, $n \geq 5$, and we find that $\begin{matrix}4\\8\end{matrix}$ is a winning 5-state. Continuing, we find that $\begin{matrix}4\\8\\36\end{matrix}$ is a winning 8-state. This is quite a bit better than we had bargained for !! We knew that $\begin{matrix}3\\0\\0\end{matrix}$ is a losing 7-state, and were inquiring merely as to whether it is a winning 8-state. We find that not only can we put 4(>3) words on top, but a sizeable number of additional words may be added at the lower levels. If we continue this investigation, we find that $\begin{matrix}4\\8\\36\\152\end{matrix}$ is a winning 11-state. Further extensions of this sequence are found in the first column of the table of Fig. 4-8, on page 142. There immediately arises the question of whether this process can be continued indefinitely, or whether this fortunate behavior for small n is merely a luck fluke. We shall show that the former situation prevails, and that in this case our faith in the orderliness of the universe is justified.

Construction of the Table in Fig. 4-8 and Proof of its Principle Properties

Contrary to our usual philosophy of exposition, at this point we temporarily resort to an axiomatic development. The preceding discussion (hopefully) has clarified the motives behind these manipulations. Lest the reader lose sight of our immediate objectives, all the results we shall now derive have been summarized and

listed beneath Fig. 4-8 at the end of this section. page 142.

Definition: The values in the table are defined recursively as follows: The first two rows are postulated as initial conditions:

$$A_{1,1} = 4;\ A_{1,2} = 2;\ A_{1,k} = 1 \quad \text{for } k \geq 3.$$

$$A_{2,1} = 8;\ A_{2,2} = 6;\ A_{2,3} = 4;\ A_{2,4} = 1;\ A_{2,k} = 0 \text{ for } k \geq 5$$

The remainder of the table is derived recursively by the following rules; applicable only when $i \geq 3$.

$$\text{For } j \geq 3,\ A_{i,j} = A_{i-1,j-1} + A_{i-1,j-2}$$

$$\text{For } j = 2,\ A_{i,2} = A_{i,3} + A_{i-1,1}$$

$$\text{For } j = 1,\ A_{i,1} = A_{i,2} + A_{i,3}$$

Definition: The state $\underline{A}_{m,j} = \begin{matrix} A_{1,j} \\ A_{2,j} \\ \cdots \\ A_{m,j} \end{matrix}$

Theorem: For $j \leq 3 \leq i$, $A_{i,j} = 2\left(\left((1+5^{1/2})/2\right)^{3i-j-2} + 2\left((1-5^{1/2})/2\right)^{3i-j-2}\right.$

Proof: Notice that the first three columns are defined only in terms of themselves. We introduce the single sequence a_k by the transformation:

$$a_k = A_{(k+3)/3,\,1} \text{ iff } k \equiv 0 \bmod 3$$

$$a_k = A_{(k+4)/3,\,2} \text{ iff } k \equiv 2 \bmod 3$$

$$a_k = A_{(k+5)/3,\,3} \text{ iff } k \equiv 1 \bmod 3$$

The recurrence relations defining $A_{i,j}$ then become

$$a_k = a_{k-1} + a_{k-2}, \quad \text{valid for } k \geq 4$$

The general solution of this equation is of the form

$$a_k = B\, r_1^k + C\, r_2^k$$

where B and C are constants determined by the two initial conditions, $a_2 = 6$ and $a_3 = 8$. r_1 and r_2 are the roots of the equation

$$r^2 = r+1$$

Solving gives $r = (1 \pm 5^{1/2})/2$, $B = C = 2$.

Transforming back from the a_k to the $A_{i,j}$ gives the desired result. Q. E. D.

Corollary:. This theorem also holds in the extended range $i \geq j$, $i \geq 3$.

Proof: These values are obtained by the same recurrence relations as their counterparts in the first three columns, to which they must be equal.

Theorem: $\underline{A}_{m,j}$ can be reduced to $\underline{A}_{m-1,j-2}$ and $\underline{A}_{m,j+1}$

Proof: We first patch up the exceptional columns on the left boundary, for $j \leq 2$, by defining $\underline{A}_{m-1,0} = \underline{A}_{m,3}$; $\underline{A}_{m-2,-1} = \underline{A}_{m,2}$.

The recurrence relations defining the table are then uniformly stated for all $m \geq 0$.

The proof consists of verifying conditions 2) and 3) of the partitioning theorem.

Condition 2) becomes

$$A_{i,j} + A_{i-1,j} = A_{i,j+1} + A_{i-1,j-2}$$

If $i = 1$ or 2, we observe that this condition is satisfied by the initial conditions. For larger i, we have

$$A_{i,j} = A_{i-1,j-1} + A_{i-1,j-2}$$

$$A_{i,j+1} = A_{i-1,j} + A_{i-1,j-1}$$

Subtraction of these two equations yields condition 2).

A sufficient condition for satisfying 3) is

$$y_{2i+2} \leq z_{2i+1} \leq y_{2i} \text{ and } z_{2i+2} \leq y_{2i+1} \leq z_{2i}$$

In the present situation this condition becomes

$$A_{i-2,j-2} \leq A_{i,j+1} \leq A_{i,j+2}$$

The latter inequality follows from the fact that $A_{i,j}$ is a monotonic nonincreasing function of j, for any fixed i. This monotonicity may be established by induction on i and the observation that the monotonicity holds for $j \leq 3$, where $A_{i,j}$ is given by an explicit formula.

The former inequality is verified as follows:

$$A_{i,j+1} = A_{i-1,j} + A_{i-1,j-1} \geq A_{i-1,j} = A_{i-2,j-1} + A_{i-2,j-2} \geq A_{i-2,j-2} \quad \text{Q.E.D.}$$

Corollary: $\underline{A}_{m,j}$ is a winning (3m-j)-state. (proof by induction).

Corollary: $V_{3m-j}(\underline{A}_{m,j}) = 2^{3m-j}$ (proof by induction, using conservation of volume theorem).

This concludes our proof of the remarkable properties of the table of Fig. 4-8, p. 142.

We can use the first column of this table to obtain a lower bound on f and R for large N. The manipulations are simple:

$$2^k \leq 2\,((1+5^{1/2})/2)^{3(j-1)} = A_{j,1} \quad \text{(to the nearest integer)}$$

so if $$k-1 \leq (j-1)\ 3 \log ((1+5^{1/2})/2)$$

we have

$$\underline{I} \leq \underline{A}_{e+j,\,1} \text{ which is a winning } 3(e+j-1)\text{-state}$$

Thus we may protect 2^k words from e errors by N questions if

$$k-1 \leq (n-3e) \log ((1+5^{1/2})/2)$$

$$R \leq (1-3f)\, R_o \; ; \; R_o = \log ((1+5^{1/2})/2)$$

Since this is identical to the line we obtained as an upper bound on R, we conclude that for all rates in the region $0 < R < R_t = .30$, (or equivalently, for all error fractions $.19 = f_t < f = e/N \leq f_o = 1/3$) this straight line gives the best possible asymptotic result. For higher rates (or lower error fractions), however, the bounds differ. The upper bound on R and f departs from the straight line and follows the curve 1-H(f). The lower bound obtained by this simple comparison with the first column of Fig. 4-8, p. 142, unfortunately, remains on the straight line for small error fractions, f.

We soon decide that in the region of this discrepancy it is the straight line, rather than the volume curve, which is the weak bound. Among other observations, we know from Gilbert's (1952) bound for one-way codes that it is possible to get the rate R up to 1 for sufficiently small error fractions f. We are thus goaded to find other sequences of winning states which provide better achievable bounds for high rates.

In this region the restraining limits are imposed by the volume bound rather than the translation bound. Intuition suggests that we would do well to construct infinite sequences of winning states which build up more slowly, having fewer nonzero components,but much greater weight. These bottommore components must carry the load for small e/N. These desires can be fulfilled by requiring that the translate of a borderline winning n-state be a borderline winning (n-4)-state instead of an

(n-3)-state. The attempt to construct a table with this property proves successful. The result is shown in Fig. 4-9 at the end of this section.

In fact, for any integer $t \geq 3$, we can compute a similar table of winning states. The first two lines of this table are defined as

$$2^{t-1} \ldots \; 2^{t-u} \qquad \ldots \; 1 \; \ldots \; 1 \; \ldots \; 1\;1\;1\;1\;1 \ldots$$

$$2^{t-1}(2^t-2t) \ldots \; 2^{t-u}(2^t-2t+u-1) \ldots \; 2^t-t-1 \ldots \; 2^v-v-1 \ldots \; 11\;4\;1\;0\;0 \ldots$$

The remainder of the table is recursively defined to fulfill the relation

$$A_{i,j} + A_{i-1,j} = A_{i,j+1} + A_{i-1,j-(t-1)}$$

This definition cinches condition 2) of the partitioning theorem. Condition 3) of the partitioning theorem is readily verified by methods similar to those illucidated for the special case t = 3. This then proves that the constructed table has the basic property:

$$\underline{A}_{m,j} \text{ reduces to } \underline{A}_{m,j+1} \text{ and } \underline{A}_{m-1,j-(t-1)}$$

To compute the rate of exponential growth of the components of the first column of this table, we can again change variables to a_k. The first t columns then become

$$a_t \; a_{t-1} \; \cdots \; a_1$$

$$a_{2t} a_{2t-1} \ldots \; a_{t+1}$$

$$a_{3t} a_{3t-1} \cdots \; a_{2t+1}$$

In terms of the a_k, the recursion relation becomes

$$a_k + a_{k-t} = 2\, a_{k-1}$$

from which we get an algebraic equation for the growth rate r

$$r^t + 1 = 2r^{t-1}$$

The growth rate of the first column, $s = r^t$, satisfies the equation

$$s + 1 = 2s^{(t-1)/t}$$

In terms of s, the achievable asymptote becomes

$$s^k \leq B\, s^j \; ; \; j + e \leq nt$$

$$k \leq (nt-e) \log s$$

$$R \leq (t-f) \log s$$

Comparing these equations with those derived in the section on tangents to the volume bound (page 131), we note that they are identical!! This bound is a straight line, emanating from the point $f_o = 1/t$ (or equivalently, $r_o = (t-1)/t$) and proceeding up to a point where it touches the volume bound tangentially, and then continues on to the R axis. For lower and lower rates, the best bounds result from higher and higher values of the integer t. The envelope of all these straight line bounds is indicated on the graph on page 119.

Attempts to eradicate the small gaps remaining at high rates between the volume bound and the achievable bounds have been as yet unsuccessful. If it were possible to devise tables of winning states which gave rise to straight lines emanating from arbitrary rational points (not restricted to the form $f_o = 1/$ integer), the problem would be solved. It is strongly conjectured that such states exist, although as yet we have not been able to demonstrate them. The case $f_o = 2/7$ has been examined at some length. The desired recursion relations are known, and they coincide with the roots of the

equation for the line tangent to the volume curve and passing through the point $f_o = 2/7$. Unfortunately, however, no successful scheme for assigning the initial values on the table has been devised.

Figure 4-8

INFINITE SEQUENCE OF BORDERLINE WINNING STATES

Column:	1	2	3	4	5	6	7	8	9	10	11	12	13	14 ...
row														
1	4	2	1	1	1	1	1	1	1	1	1	1	1	1
2	8	6	4	1	0	0	0	0	0	0	0	0	0	0
3	36	22	14	10	5	1	0	0	0	0	0	0	0	0
4	152	94	58	36	24	15	6	1	0	0	0	0	0	0
5	644	398	246	152	94	60	39	21	7	1	0	0	0	0
6	2728	1686	1042	644	398	246	154	99	60	28	8	1	0	0
7	11556	7142	4414	2728	1686	1042	644	400	253	159	88	36	9	1
.														
.														
.														

MOST IMPORTANT PROPERTIES

Let A_{ij} be the number in the i^{th} row and the j^{th} column: $\underline{A}_{m,j} = \begin{matrix} A_{1,j} \\ A_{2,j} \\ \cdots \\ A_{m,j} \end{matrix}$

$\underline{A}_{m,j}$ is a borderline winning $(3m-j)$-state. It satisfies volume bound with equality. It can be reduced to $\underline{A}_{m,(j+1)}$ and $\underline{A}_{(m-1),(j-2)}$

$$A_{i,j} + A_{i,(j+1)} = A_{(i+1),(j+2)} \qquad \text{(unless } i \leq 2\text{)}$$

If $i \geq j$ and $i \geq 3$, then

$$A_{i,j} = 2((1+5^{1/2})/2)^{3i-j-2} + 2((1-5^{1/2})/2)^{3i-j-2}$$

Figure 4-9

ANOTHER INFINITE SEQUENCE OF BORDERLINE WINNING STATES

8	4	2	1	1	1	1	1	1	1	1
64	36	20	11	4	1	0	0	0	0	0
744	404	220	120	67	35	16	5	1	0	0
8512	4628	2516	1368	744	407	222	118	22	6	1

Concluding remarks

The partitioning strategy of Fig. 4-8 has asymptotically optimum error correction capability at all rates less than . 2965 bits/bit. At that rate its error exponent is asymptotically optimum on any binary symmetric channel with any transition probability, p. At this rate, this strategy is asymptotically a perfect code.

The other, similar strategies described in the previous section are each perfect at some other particular rate, given by the corresponding tangent to the volume bound as shown in Fig. 4-4, p. 119.

By examining the properties of these strategies, the weaknesses of our initial simpleminded probability strategies and order strategies are evident. The probability strategies fail because they are too eager to play everything else against the top word; the order strategies, because they are too reluctant. The optimum strategies of Figs. 4-8 and 4-9 are quite flexible in their method of handling this problem. If the top word is near the surface of the pack, very few words are played against it. As it rises above the pack, however, more and more words are played against it. This either forces the top word to come back down or it further depresses the level of the surface of the pack, thus avoiding the disastrous phenomenon of Fig. 4-2, p. 114.

The optimum strategies do not depend on the capricious channel probability, p. Since in many applications this parameter is imprecisely known, this property is a real advantage. Conversely, the strong dependence on p is one of the primary reasons why probability strategies fail. When a decoding error occurs, the frequency of channel errors over the undecodable block is given by p', a tilted probability which is always greater than p. By bisecting probabilities based on p, the probability strategies are fighting straw men and ignoring the real dangers.

At rates below .2965 bits/bit, we do not know whether the strategies of Fig. 4-8 have optimum error exponent or not. They do have optimum error correction capability, but as we showed in the second section of this chapter, this is equivalent to optimum error exponent only in the limit of infinitesmal channel error probability, p.

At these low rates, the real problem with the strategies computed from the table of Fig. 4-8 is that they are imprecisely defined. For example, suppose we start with $M = 8,192 = 2^{13}$ codewords, which we wish to protect against all patterns of 50 or fewer errors. From Fig. 4-8 we deduce that this can be accomplished in 169 questions since

$$\begin{matrix} 2 & & 0 \\ 6 & & 0 \\ 22 & & 0 \\ 94 & & 0 \\ 398 & > & 0 \\ 1686 & & 1042 \\ 7142 & & 7142 \\ \cdots & & 0 \\ & & \cdots \\ A_{57,1} & & 0 \end{matrix}$$

The former is a winning 169-state, and Lemmas 4 and 4′ apply. But how do we partition this state? The table says only that it should be partitioned in such a way that it is dominated by

$$\begin{matrix} 0 \\ \cdots \\ 0 \\ 1042 \\ 4414 \\ 0 \\ \cdots \end{matrix}$$

There are many partitions that do that. At every subsequent question, we will have similar options. Depending on which options we choose, we may be victorious over almost all patterns of 51, 52, and 53 errors, or we may concede defeat to most patterns of only 51 errors.

Basic improvement of the results of this chapter can result only from constructing explicit algorithms for determining good partitions, not from the construction of additional tables. As far as they go, our tables are as good as possible.

Appendix A

A STRONG CONVERSE TO CHERNOV'S BOUND

Introduction: Chernov bounds are used to bound the probability that the sum of a large number of random variables is significantly larger than their average. For identically distributed independent random variables, (the only case considered here), Chernov gives an upper bound to the probability that the sum of the n random variables is substantially larger than expected. The bound decreases exponentially in n:

$$\Pr\left(\sum_{i=1}^{n} z_i \geq nZ_o\right) \leq \exp -nE$$

where z_i is a random variable with probability distribution P(z); Z_o is any fixed number such that $Z_o > \bar{Z} = \int z\, P(z)\, dz$; and E is Chernov's exponent (dependent on Z_o and P(z)).

The direct converse to Chernov's bound states that in fact this bound is exponentially optimum:

$$\lim_{n\to\infty} -1/n \log \Pr\left(\sum_{i=1}^{n} z_i \geq nZ_o\right) = E$$

The proof of Chernov's bound follows directly from a few simple manipulations with moment-generating functions; the proof of the converse involves application of the Central Limit Theorem or Chebycheff's inequality to a tilted probability distribution† derived from P(z). Further discussion of these points can be found in several places (for example, see Appendix B of Gallager: Low Density Parity-Check Codes), and we will not give any further details here.

The theorem which we prove here is stronger than the direct converse of Chernov's bound. It states that not only will $\sum_{i=1}^{n} z_i \geq nZ_o$, with a probability which is exponentially E, but all partial sums will similtaneously be that large with the same exponential probability.

(†) Tilted probabilities were apparently first introduced by Feller (1943)

Theorem:

$$\lim_{n\to\infty} -1/n \ln \Pr\left(\sum_{i=1}^{k} z_i \geq kZ_o \text{ for all } k \leq n\right) = E = \lim_{n\to\infty} -1/n \ln \Pr\left(\sum_{i=1}^{n} z_i \geq nZ_o\right) \quad \text{A.01}$$

Proof: Without loss of generality. we assume that $\bar{z} = 0; Z > 0$ A.02

Suppose it is possible to select some $Z_1 > Z_o$ such that Z_1 has a greater Chernov exponent than Z_o:

$$\lim_{n\to\infty} -1/n \Pr\left(\sum_{i=1}^{n} z_i \geq nZ_1\right) = E'; \; E < E' < \infty \quad \text{A.03}$$

If no such Z_1 exists, then the theorem is trivial. If such a Z_1 exists, then we can choose non-negative, integral-valued monotonic functions M(n) and m(n) such that

$$M(Z_1 - Z_o) \geq Z_1 \quad \text{A.11}$$

$$\lim_{n\to\infty} m = \lim M = \infty \quad \text{A.12}$$

$$\lim_{n\to\infty} n/m = \lim_{n\to\infty} n/m = \infty \quad \text{A.13}$$

$$\text{For any fixed } E > 0, \lim_{n\to\infty} n \exp -mE = 0 \quad \text{A.14}$$

For example, one might choose $m(n) = n^{1/2}$, rounded up or down.

The theorem mentions the event that

(*1) $\sum_{i=1}^{k} z_i \geq kZ_o$ for all $k \geq n$

Our proof introduces several other events

$$(*1_I) \qquad \sum_{i=1}^{I} z_i \geq IZ_o$$

$$(*1_I') \qquad \sum_{i=1}^{I} z_i < IZ_o$$

$$(*1') = \bigcup_{I=1}^{n} (*1_I')$$

Note that (*1') is the complement of (*1)

$$(*2_i) \qquad z_i \geq z_1$$

$$(*2) = \bigcap_{i=1}^{M} (*2_i)$$

$$(*3_j) \qquad \sum_{i=M+(j-1)m+1}^{M+jm} z_i \geq mz_o$$

$$(*3) = \bigcap_{j=1}^{[(n-M)/m]^*} (*3_j)$$

$$(*4_I) \qquad \sum_{i=I+1}^{dm+M} z_i \geq mz_I$$

where $1 \geq dm + M - I \leq m$

We shall show that (*3) has the desired exponent, that (*2) is sufficiently probable that it can be assumed without exponential loss, and that together the events (*2) and (*3) virtually assure (*1).

Since (*1) implies $(*1_n)$,

$$\lim_{n\to\infty} -1/n \ \ln \ Pr\ (*1) \geq E \qquad \text{A.20}$$

On the other hand, since (*2) and (*3) are independent events, Baye's Rule becomes

$$\ln Pr\ (*1) \geq \ln Pr\ (*1 \ \& \ *2 \ \& \ *3)$$

$$= \ln Pr\ (*2) + \ln Pr\ (*3) + \ln Pr((*1)/*2+*3) \qquad \text{A.21}$$

Our goal is to show that in the limit this equation is

$$\lim_{n\to\infty} -1/n \ln Pr\ (*1) \leq 0 + E + 0 \qquad \text{A.22}$$

A.22 and A. 20 will them prove the theorm.

We verify the claims term by term.

$$(*1') = \bigcup_{I=1}^{n} (*1_I')$$

Note that (*1') is the complement of (*1)

$$(*2_i) \qquad z_i \geq Z_1$$

$$(*2) = \bigcap_{i=1}^{M} (*2_i)$$

$$(*3_j) \qquad \sum_{i=M+(j-1)m+1}^{M+jm} z_i \geq mZ_o$$

$$(*3) = \bigcap_{j=1}^{[(n-M)/m]^*} (*3_j)$$

$$(*4_I) \qquad \sum_{i=I+1}^{dm+M} z_i \geq mZ_I$$

where $1 \geq dm + M - I \leq m$

We shall show that (*3) has the desired exponent, that (*2) is sufficiently probable that it can be assumed without exponential loss, and that together the events (*2) and (*3) virtually assure (*1).

Since (*1) implies $(*1_n)$,

$$\lim_{n\to\infty} -1/n \ \ln \ Pr\ (*1) \geq E \qquad \text{A.20}$$

On the other hand, since (*2) and (*3) are independent events, Baye's Rule becomes

$$\ln Pr\ (*1) \geq \ln Pr\ (*1\ \&\ *2\ \&\ *3)$$

$$= \ln Pr\ (*2) + \ln Pr\ (*3) + \ln Pr((*1)/*2*3) \qquad \text{A.21}$$

Our goal is to show that in the limit this equation is

$$\lim_{n\to\infty} -1/n \ln Pr\ (*1) \leq O + E + O \qquad \text{A.22}$$

A.22 and A. 20 will them prove the theorm.

We verify the claims term by term.

First term:

$$\ln \Pr(*2) = \sum_{i=1}^{M} \ln \Pr(*2_i) = M \ln \Pr(z \geq Z_1) \qquad \text{A. 30}$$

$$\lim_{n\to\infty} -1/n \ln \Pr(*2) = 0, \text{ by A.13} \qquad \text{A .31}$$

Second term:

$$\ln \Pr(*3) = \sum_{j} \ln \Pr(*3_j) = (n-M)/m \ln \Pr\left(\sum_{i=1}^{m} z_i \geq mZ_o\right) \qquad \text{A.32}$$

$$\lim_{n\to\infty} -1/n \ln \Pr(*3) = \lim_{n\to\infty} (1-M/n)\left(-1/m \ln \Pr\left(\sum_{i=1}^{m} z_i \geq mZ_o\right)\right) \qquad \text{A. 33}$$

$$= \lim_{n\to\infty} \left(-1/m \ln \Pr\left(\sum_{i=1}^{m} z_i \geq nz_o\right)\right) = E \qquad \text{A. 34}$$

For any j, we have $\Pr(*3_j) = \exp -m\,(E - o(m))$ where $o(m)$ goes to zero as m goes to ∞. A. 35

Third term:

We first claim that $(*1'_I \;\&\; *2 \;\&\; *3)$ implies $(*4_I)$

Proof: Using the division algorithm,

$I-M = dm - r$, determining the integers d and r A. 40

with $0 < r \leq m$. Then if $(*1'_I \;\&\; *2 \;\&\; *3)$ occurs,

$$\sum_{i=1}^{I} x_i < IZ_o \qquad \text{by } *1'_I \qquad \text{A. 41}$$

$$\sum_{i=1}^{M} z_i \geq MZ_1 \qquad \text{by } *2 \qquad \text{A. 42}$$

$$\sum_{i=M+1}^{M+dm} z_i \geq dmZ_o \qquad \text{by } *3 \qquad \text{A. 43}$$

$$\sum_{i=I+1}^{dm+M} z_i \geq (dm - I)Z_o + MZ_1 \text{ (by A.43 + A.42 - A.41)} \qquad \text{A. 44}$$

$$= (r-M)Z_o + MZ_1 \qquad \text{by A.40} \qquad \text{A. 45}$$

$$= rZ_o + M(Z_1 - Z_o) \qquad \text{A. 46}$$

$\geq M(Z_1 - X_o)$ by A. 02 A. 57

$\geq mZ_1$ by A. 11 A. 58

So, $Pr(*1_I'/*2 \ \&*3) \leq Pr\ (*4_I/*2\ \&\ *3)$ by A. 40 to A. 48 A. 50

$= Pr\ (*4_I/*3_d)$ A. 51

because *2 and *3j are independent of $*4_I$ for all j =d.

Continuing,

$$Pr\ (*4_I/*3_d) = Pr\ (*4_I\ \&\ *3_d) / Pr\ (*3_d)$$

$$\leq Pr\ (*4_I) / Pr\ (*3_d) \qquad \text{A. 52}$$

We wish to bound $Pr\ (*4_I)$.

Since $\bar{z} = 0$, the central limit theorem assures us that

$$\lim_{n \to \infty} Pr\ \left(\sum_{i=1}^{n} z_i \geq 0 \right) \geq 1/2 \qquad \text{A. 60}$$

And since $Pr\ (z \geq 0) > 0$ A. 61

we may define

$$P_o = \min_k Pr\ \left(\sum_{i=1}^{k} z_i \geq 0 \right) > 0 \qquad \text{A. 62}$$

Then

$$Pr\ \left(\sum_{i=r+1}^{m} z_i \geq 0 \right) \geq P_o \qquad \text{A. 63}$$

Notice that

$$\left(\sum_{i=1}^{r} z_i \geq mZ_1 \right) \ \&\ \left(\sum_{i=r+1}^{m} z_i \geq 0 \right) \text{ implies } \left(\sum_{i=1}^{m} z_1 \geq mZ_1 \right) \qquad \text{A. 64}$$

so

$$Pr\ \left(\sum_{i=1}^{r} z_1 \geq mZ_1 \right) \leq Pr\ \left(\sum_{i=1}^{m} z_i \geq mZ_1 \right) / Pr\ \left(\sum_{i=r+1}^{m} z_i \geq 0 \right) \qquad \text{A. 65}$$

$$Pr\ \left(\sum_{i=1}^{r} z_i \geq mZ_1 \right) \leq 1/p_o \sum_{i=1}^{m} \exp -mE' \quad \text{by A. 63 and Chernov} \qquad \text{A. 66}$$

Translating z_i in A. 66 into z_{I+i} gives

$$Pr\ (*4_I) \leq 1/p_o \ \exp - mE' \qquad \text{A. 67}$$

Combining A.67 with A,52 and A.35 gives

$$\Pr\ (*4_I/*3_d) \leq 1/p_p \quad \exp -m(E'-E+ o(m)) \qquad \text{A.90}$$

Invoking A.50 and the definition of (*1') gives

$$\Pr\ (*1'/*2\ \&\ *3) \leq (* (n-M)/p_o \quad \exp -m\ (E' - E= o(m)) \qquad \text{A.91}$$

since the probability of the union of events is overbounded by the sum of probabilities. Applying A.14 to A.91 gives

$$\lim_{n\to\infty} \Pr\ (*1'/*2\ \&\ *3) = 0 \qquad \text{A.92}$$

$$\lim_{n\to\infty} \Pr(*1/*2\ \&\ *3) = 1 \qquad \text{A.93}$$

$$\lim_{n\to\infty} \ln\ \Pr\ (*1/*2\ \&\ *3) = 0 \qquad \text{A.94}$$

Comments: The general proof just given makes no attempt to optimize the coefficient. It is felt that the probability of all partial sums being large is roughly 1/n times the probability that only the final nth sum will be large. For certain cases, such as the case of binary variables assuming the values 1 and 0 with probability one half each, such problems have been studied extensively under the name of ballot problems. This terminology arises from applications to election night, when one wishes to know the probability that the candidate currently ahead will remain ahead throughout the counting and eventually win.

Except for a factor of 2^n, the ballot problem is the same as the second of the two following combinatorial problems: How many ways are there of putting k balls into n cells, with no more than one ball/cell? How many of these ways satisfy the additional condition that for any j, the first j cells contain at least jk/n balls?

The answer to the first question is well-known to be $\binom{n}{k}$. The answer to the second question has been computed by Takacs(1962) It is a complicated expression, except in certain special cases. For example, if n and k are relatively prime, the answer if $\binom{n}{k}/n$; if n = 2k, the answer is the "Catalan number," $\binom{n}{k}/(n-k+1)$.

Additional results on ballot problems are given by Riordan (1964), and Graham (1963).

BIBLIOGRAPHY

	Page cited(†)
Berlekamp, E. R. (1962) "Machine Solution of No-Trump Double Dummy Bridge Problems," MS Thesis, MIT EE Department	B
Berlekamp, E. R. (1963) "A Class of Convolution Codes," Information and Control, 6, 1-13.	B
Berlekamp, E. R. (1963) "Program for Double Dummy Bridge--A New Strategy for Mechanical Game Playing" Journal of the Association for Computing Machinery, 10, 357-364	B
Berlekamp, E. R. (1963) "The Game of Black" Mathematical Games Department of Scientific American, October & November	B
Berlekamp, E. R. (1963) "Probabilistic Mazes" (Presently Unpublished)	B
Berlekamp, E R. (1963) "The Enumeration of Matrices by Rank" (Presently Unpublished)	B
Berlekamp, E. R. (1963) "On the Minimum Number of Questions to Determine a Subset of a Given Set" (Publication Rejected because of simultaneous solution by P. Erdos)	B
Berlekamp, E. R. (1964) "Note on Recurrent Codes" PGIT, July	B
Berlekamp, E. R., & E. N. Gilbert & F. W. Sinden (1964 or 1965) "A Polygon Problem" to appear in American Mathematical Monthly	B
Berlekamp, E. R. (1965). See Shannon, C. E.	6,10, 36,44, 106
Bose, R. C. (1947) "Mathematical Theory of the Symmetrical Factorial Design," Sankhya 8, 107-166	9
Bose, R. C. & D. K. Ray-Chaudhuri, (1960) "On a Class of Error Correcting Binary Group Codes," and "Further Results on Error Correcting Binary Group Codes," Information & Control, 3,68-79 & 279-290.	104
Cauchy, A. L. (1821) "Analyse Algebrique" Cours d'analyse de l'Ecole Royale Polytechnique. Ire partie.	30

(†) Those papers not cited in the text, but which are listed to satisfy the requirement that all papers by the author be mentioned in the biography, are marked B.

BIBLIOGRAPHY
(continued)

	page
Chang, S. S. L. (1956) "Theory of Information Feedback Systems," PGIT, IT2, 29-40.	7
Chaudhuri, D. K. R. See Bose, R. C.	104
Chernov, H. (1952) "A Measure of Asymptotic Efficienty for Tests of an Hypothesis Based on the Sum of Observations," Annuls of Math. Stat. 23 493-	146
Dobrushin, R. L. (1962) "Optimal Binary Codes for Small Rates of Transmission of Information," Theory of Probability and its Applications, 7, 199-204	6,16, 23, 90
Elias, P. (1955) "List Decoding for Noisy Channels," Technical Report 335, RLE. Also Wescon Convention Record	101
Elias, P. (1963) See Gramenopoulos, N.	6, 118
Fano, R. M. (1961) Transmission of Information, MIT Press.	2,3 16 73
Fano, R. M. (1963) "A Heuristic Discussion of Probabilistic Decoding" PGIT, IT9, 64-74.	5
Feinstein, A. (1954) "A New Basic Theorem of Information Theory," PGIT-4, 2-	2
Feinstein, A. (1955) "Error Bounds in Noisy Channels Without Memory," PGIT, IT-1, 13-14	2
Feller, W. (1943) "Generalization of a Probability Limit Theorem of Cramer," Transactions of the American Mathematical Society, 54, 361-	146
Feller, W. (1950) An Introduction to Probability Theory and Its Applications John Wiley & Sons	63
Gallager, R. G. (1963) Low Density Parity-Check Codes, MIT Press	146
Gallager, R. G. (October 1964 or January 1965) "A Simple Derivation of the Coding Theorem and Some Applications," PGIT, IT 11	3,5,15,19 35,64,101 106
Gallager, R. G. (1965) See Shannon, C. E.	6,10,36 44,106
Gardner, M. (October & November, 1963) "Mathematical Games" Scientific American	B

BIBLIOGRAPHY (Continued)

	page cited
Gilbert, E. N. (1952) "A Comparison of Signalling Alphabets," BSTJ 31, 504-522.	118 139
Gilbert, E. N. (1964). See Berlekamp, E. R.	B
Gleason, A. M. (1963) Private Communications.	105
Graham, R. L. (1963) "A Combinatorial Theorem for Partial Sums" Annals of Math. Stat. 34 1600-1602	152
Gramenopoulos, N. (1963) "An Upper Bound for Error Correcting Codes," MS Thesis, EE Department, MIT.	6 118
Hall, M. (1958) "A Survey of Combinatorial Analysis" in Some Aspects of Analysis and Probability, by Kaplansky, Hall, Hewitt, and Fortet. Wiley & Sons	9
Hamming, R. W. (1950) "Error Detecting and Error Correcting Codes" BSTJ 29, 47-160	104,118 126,129
Hardy, G. H. & J. E. Littlewood & G. Polya (1934) Inequalities Cambridge University Press	30
Horstein, M. (1963) "Sequential Transmission Using Noiseless Feedback," PGIT, IT9 136-143	7 110
Littlewood, J. E. (1934) See, Hardy, G. H.	30
MacWilliams, Mrs. F. J. (1962) "A Theorem on the Distribution of Weights in a Systematic Code" BSTJ 42, 79-94	105
MacWilliams, Mrs. F. J. (1964) "Permutation Decoding" BSTJ January	B
Mann, H. B. (1949) Analysis and Design of Experiments, Dover Publications, N.Y.	9
Mattson, H. F. & G. Solomon (1961) "A New Treatment of Bose-Chaudhuri Codes," Journal of the Society for Industrial Applied Mathematics, 9, 655-669	104
Niven, I. (1963) Diophantine Approximations Wiley & Sons	22
Peterson, W. W. (1961) Error-Correcting Codes, MIT Press	47
Pless, Miss V. (1963) "Power Moment Identities on Weight Distributions in Error Correcting Codes" Information & Control, 6, 147-152	105

BIBLIOGRAPHY
(continued)

	page cited
Plotkin, M (January, 1951) Research Division Report 51-20, University of Pennsylvania. Eventually published in 1960 as "Binary Codes with Specified Minimum Distance," PGIT, IT 6, 445-450.	6,17 105 107 118
Polya, G (1934) See Hardy, G. H.	30
Prange, E. (September, 1957) Cyclic Error-Correction Codes in Two Symbols, AFCRC-TN-57-103, Air Force Cambridge R. Ce	104
Reed, I. S. (1954) "A Class of Multiple-Error-Correcting-Codes and the Decoding Scheme" PGIT-4 38-49	77
Reiffen, B. (1961) See Wozencraft, J. M.	5
Reiffen, B. (1963) "A Note on 'Very Noisy' Channels" Information & Control, 6, 126-130	9 33,106
Riordan, J. (1964) "The Enumeration of Election Returns by Number of Lead Positions" Annals of Math. Stat. 35,369-379.	152
Ryser, H. J. (1963) Combinatorial Mathematics Carus Monograph, Wiley & Sons	9
Shannon, C. E. & W. Weaver (1949) Mathematical Theory of Communication, U. of Illinois Press, Urbana	3
Shannon, C. E. (1956) "Zero-Error Capacity of Noisy Channels" PGIT, IT2, 8-	3 11
Shannon, C. E. (1959) "Probability of Error for Optimal Codes in a Guassian Channel," BSTJ 38, 611-	3
Shannon, C. E. (1964) Private Communications	43 101
Shannon, C. E. & R. G. Gallager, & E. R. Berlekamp, (1965). Forthcoming paper, probably to appear in PGIT. Will prove the new straight line upper bound and much of Chapter 2 of this thesis	6,10 36 44 100
Sinden, F. W. (1964) See Berlekamp, E. R.	B

BIBLIOGRAPHY
(continued)

	page cited
Solomon, G. (1961) See Mattson, H. F.	104
Steiner, J. (1853) "Combinatorishe Aufgabe" Crelle's Journal 45 181-182	8
Sterling, J. (1730) Methodus Differentialis	73
Takacs, L. (1962) "A Generalization of the Ballot Problem and Its Application in the Theory of Queues" American Stat. Association Journal, June, 327-337	152
Weaver, W. (1949) See Shannon, C. E.	1, 105
Wolfowitz, J. (1960) "Strong Converse of the Coding Theorem for General Discrete Finite Memory Channels" Information & Control, 3, 89-93	2
Wolfowitz, J. (1961) Coding Theorems of Information Theory, Prentice Hall	2
Wozencraft, J. M & B. Reiffen, (1961) Sequential Decoding, MIT Press.	5
Yudkin, H. L. (1964) Private Communications	40

Autobiographical Sketch

I was born on September 6, 1940, at Dover, Ohio, and lived in nearby Strasburg, Ohio, until the age of 9 when my parents moved to Fort Thomas, Kentucky, a suburb of Cincinnati, Ohio, where they still reside. My father, the Rev. Waldo Berlekamp, is a minister for the United Church of Christ. I have two brothers and one sister, Mrs. Marian Warden, who is 5 1/2 years older than I.

At the age of 10 I taught myself how to juggle, a diversion which has been one of my favorite hobbies ever since.

I attended high school at Highlands High, Fort Thomas, Kentucky. In addition to my scholastic activities there, I was active in music, sports, and school politics. I was president of the band and composed several marches, one of which I copyrighted. I helped win a state championship in swimming and was sports editor for the student newspaper and president of the senior class. Following a very interesting summer (1957) in the science and engineering division of the National High School Institute at Northwestern University, Evanston, Illinois, I decided upon a technical career and applied for admission to MIT.

Following my graduation from high school as salutatorian (due to a lone B, in Latin) of Highlands' class of 1958, I entered MIT as a freshman in September 1958, supported by a 4-year award from the National Merit Scholarship Corporation.

My first industrial experience came with the Cincinnati Milling Machine Company during the summer of 1959. I was employed as a computer programmer. I spent the summer writing a preprocessing program for numerically controlled milling machines.

In the spring of 1960 I transferred into the cooperative course in electrical engineering, a five year program which intersperses summer industrial assignments with the normal MIT course work during the winters, except for one term in the final year during which the student does his Master's thesis at the company. I took my industrial assignments at Bell Telephone Laboratories (BTL), Murray Hill, New Jersey. The first summer (1960), I extended my computer programming experience by writing a 7090 program to simulate a talking machine, under the supervision of E. E. David, Jr., and J. L. Kelly, Jr. The next summer (1961) was spent on a rather abortive assignment in the solid state electronics (transistors) research department. The major lesson I learned that summer was that I would never make a good experimental physicist.

Due to the increased pressure of academic work, my extra-curricular activities as an undergraduate at MIT were considerably curtailed from high school, and I tended more toward intellectual recreations. I won the MIT freshman chess championship (1959), the MIT Open Pairs Bridge Tournament (1960), and the New England Intercollegiate Duplicate Bridge Championship (1961). I wrote a weekly bridge column for THE TECH, MIT's newspaper. During the first term of my senior year I lived in a dormitory in which everyone spoke Russian.

In the spring of 1961, I received the Blounder-Tongue Award, a scholastic honor given annually to an MIT junior EE major. In December 1961, I won a William Lowell Putnam Award for finishing among the top five on a national intercollegiate mathematics examination sponsored by the American Mathematical Association.

Due to overloads, advanced standing examinations, and graduate subjects which I had elected while an undergraduate, I lacked only one course and a thesis of a master's degree when I was admitted to MIT's graduate school in February, 1962. I advanced stood the remaining subject, wrote my thesis while on cooperative assignment that spring and summer at BTL, and received the BS and MS degrees in electrical engineering from MIT in September, 1962.

Since then I have been enrolled in graduate studies at MIT, supported by cooperative fellowships from the National Science Foundation. During the summer of 1963 I worked on a variety of projects in the mathematical research department of BTL under the supervision of D. Slepian and H. O. Pollak. My more important papers, and certain other papers in whose preparation I have had a minor part, are listed in the bibliography. Those which are not referred to in the body of this thesis are marked "B".

This fall I shall begin teaching at the University of California at Berkeley as an assistant professor of electrical engineering.