

AD-A125 872

CODING FOR FREQUENCY-HOPPED SPREAD-SPECTRUM CHANNELS
WITH PARTIAL-BAND INTERFERENCE(U) ILLINOIS UNIV AT
URBANA COORDINATED SCIENCE LAB W E STARK JUL 82 R-945

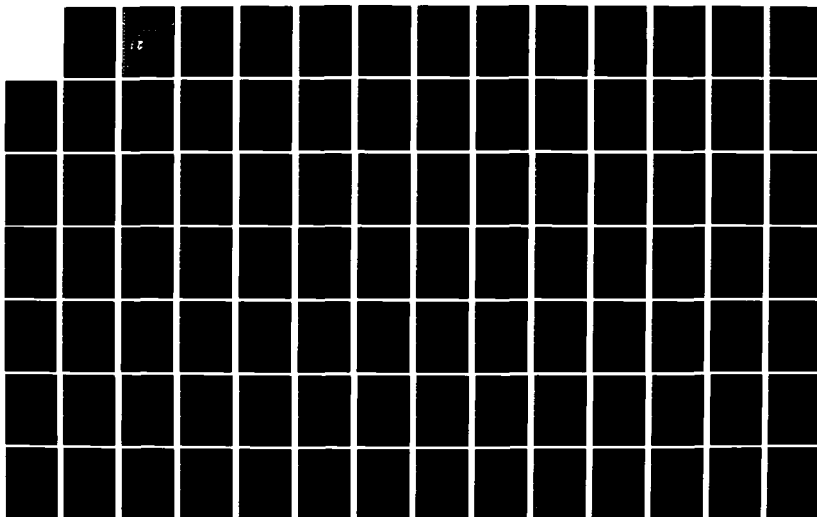
1/2

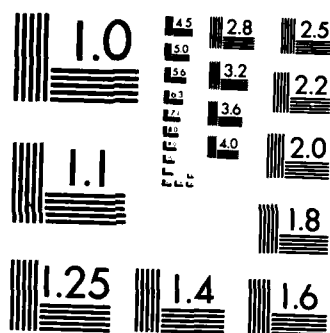
UNCLASSIFIED

N00014-79-C-0424

F/G 17/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

REPORT R-945

JULY, 1982

U1LU-ENG 82-2211

E COORDIN

LABOR

ELECTE

MAR 21 1983

A

CODING FOR FREQUENCY-HOPPED SPREAD-SPECTRUM CHANNELS WITH PARTIAL-BAND INTERFERENCE

WAYNE ERIC STARK

APPROVED FOR PUBLIC RELEASE. DISTRIBUTION UNLIMITED.

DTIC FILE COPY

AD A 125872

03 03 21 008

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO. AD-A125872	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) CODING FOR FREQUENCY-HOPPED SPREAD-SPECTRUM CHANNELS WITH PARTIAL-BAND INTERFERENCE		5. TYPE OF REPORT & PERIOD COVERED Technical Report
7. AUTHOR(s) Wayne Eric Stark		6. PERFORMING ORG. REPORT NUMBER R-945; UILU-ENG 82-2211
9. PERFORMING ORGANIZATION NAME AND ADDRESS Coordinated Science Laboratory 1101 W. Springfield Avenue University of Illinois at Urbana-Champaign Urbana, IL 61801		8. CONTRACT OR GRANT NUMBER(s) N00014-79-C-0424
11. CONTROLLING OFFICE NAME AND ADDRESS Joint Services Electronics Program		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
14. MONITORING AGENCY NAME & ADDRESS (if different from Controlling Office)		12. REPORT DATE July 1982
		13. NUMBER OF PAGES 135
		15. SECURITY CLASS. (of this report) UNCLASSIFIED
		15a. DECLASSIFICATION/DOWNGRADING SCHEDULE
16. DISTRIBUTION STATEMENT (of this Report) Approved for public release; distribution unlimited		
17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)		
18. SUPPLEMENTARY NOTES		
19. KEY WORDS (Continue on reverse side if necessary and identify by block number)		
20. ABSTRACT (Continue on reverse side if necessary and identify by block number) The performance of codes on frequency-hopped spread-spectrum channels with partial-band interference is investigated. The asymptotic performance of codes is measured by the channel capacity and the random coding exponent. The performance of specific codes is measured by the bit error probability. The channel models we consider are quite general and include channels with unknown parameters, channels which change with time, and channels with memory. These models are applicable to frequency-hopped spread-spectrum communication systems as well as to several other communication systems.		

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE(When Data Entered)

We formulate the problem of communicating over channels with unknown transition probabilities (i.e. communicating over channels with jamming) as a game theory problem with payoff function being the mutual information between the channel input and the channel output. Under certain restrictions it is shown that memoryless coding and jamming strategies are simultaneously optimal strategies. Next we develop simple, yet accurate, models for many channels with memory that arise in practice. The channel statistics are constant for blocks of symbols of fixed length. The receiver is said to have side information if it can determine the channel statistics for each block of symbols transmitted. We determine the capacity, cutoff rate, and random coding exponent for these channels. The capacity without side information is an increasing function of the memory length while the cutoff rate is a decreasing function of the memory length. We show that, for channels with memory and side information random-error correcting codes with interleaving and burst-error correcting codes have comparable performance, while for channels without side information random-error correcting codes with interleaving are inferior to burst-error correcting codes. As a particular example, we examine the performance of several forms of modulation and demodulation with partial-band jamming. Our conclusion is that partial-band jammers can be neutralized provided we use codes with rate less than a constant that depends on the form of modulation and demodulation.



A. POSITION FOR	
B. CASE	
C. DATE	
D. APPROVAL	
E. COMMENTS	
F. SIGNATURE	
G. DATE	
H. APPROVAL	
I. COMMENTS	
J. SIGNATURE	
K. DATE	
L. APPROVAL	
M. COMMENTS	
N. SIGNATURE	
O. DATE	
P. APPROVAL	
Q. COMMENTS	
R. SIGNATURE	
S. DATE	
T. APPROVAL	
U. COMMENTS	
V. SIGNATURE	
W. DATE	
X. APPROVAL	
Y. COMMENTS	
Z. SIGNATURE	
AA. DATE	
AB. APPROVAL	
AC. COMMENTS	
AD. SIGNATURE	
AE. DATE	
AF. APPROVAL	
AG. COMMENTS	
AH. SIGNATURE	
AI. DATE	
AJ. APPROVAL	
AK. COMMENTS	
AL. SIGNATURE	
AM. DATE	
AN. APPROVAL	
AO. COMMENTS	
AP. SIGNATURE	
AQ. DATE	
AR. APPROVAL	
AS. COMMENTS	
AT. SIGNATURE	
AU. DATE	
AV. APPROVAL	
AW. COMMENTS	
AX. SIGNATURE	
AY. DATE	
AZ. APPROVAL	
BA. COMMENTS	
BB. SIGNATURE	
BC. DATE	
BD. APPROVAL	
BE. COMMENTS	
BF. SIGNATURE	
BG. DATE	
BH. APPROVAL	
BI. COMMENTS	
BJ. SIGNATURE	
BK. DATE	
BL. APPROVAL	
BM. COMMENTS	
BN. SIGNATURE	
BO. DATE	
BP. APPROVAL	
BQ. COMMENTS	
BR. SIGNATURE	
BS. DATE	
BT. APPROVAL	
BU. COMMENTS	
BV. SIGNATURE	
BW. DATE	
BX. APPROVAL	
BY. COMMENTS	
BZ. SIGNATURE	
CA. DATE	
CB. APPROVAL	
CC. COMMENTS	
CD. SIGNATURE	
CE. DATE	
CF. APPROVAL	
CG. COMMENTS	
CH. SIGNATURE	
CI. DATE	
CJ. APPROVAL	
CK. COMMENTS	
CL. SIGNATURE	
CM. DATE	
CN. APPROVAL	
CO. COMMENTS	
CP. SIGNATURE	
CQ. DATE	
CR. APPROVAL	
CS. COMMENTS	
CT. SIGNATURE	
CU. DATE	
CV. APPROVAL	
CW. COMMENTS	
CX. SIGNATURE	
CY. DATE	
CZ. APPROVAL	
DA. COMMENTS	
DB. SIGNATURE	
DC. DATE	
DD. APPROVAL	
DE. COMMENTS	
DF. SIGNATURE	
DG. DATE	
DH. APPROVAL	
DI. COMMENTS	
DJ. SIGNATURE	
DK. DATE	
DL. APPROVAL	
DM. COMMENTS	
DN. SIGNATURE	
DO. DATE	
DP. APPROVAL	
DQ. COMMENTS	
DR. SIGNATURE	
DS. DATE	
DT. APPROVAL	
DU. COMMENTS	
DV. SIGNATURE	
DW. DATE	
DX. APPROVAL	
DY. COMMENTS	
DZ. SIGNATURE	
EA. DATE	
EB. APPROVAL	
EC. COMMENTS	
ED. SIGNATURE	
EE. DATE	
EF. APPROVAL	
EG. COMMENTS	
EH. SIGNATURE	
EI. DATE	
EJ. APPROVAL	
EK. COMMENTS	
EL. SIGNATURE	
EM. DATE	
EN. APPROVAL	
EO. COMMENTS	
EP. SIGNATURE	
EQ. DATE	
ER. APPROVAL	
ES. COMMENTS	
ET. SIGNATURE	
EU. DATE	
EV. APPROVAL	
EW. COMMENTS	
EX. SIGNATURE	
EY. DATE	
EZ. APPROVAL	
FA. COMMENTS	
FB. SIGNATURE	
FC. DATE	
FD. APPROVAL	
FE. COMMENTS	
FF. SIGNATURE	
FG. DATE	
FH. APPROVAL	
FI. COMMENTS	
FJ. SIGNATURE	
FK. DATE	
FL. APPROVAL	
FM. COMMENTS	
FN. SIGNATURE	
FO. DATE	
FP. APPROVAL	
FQ. COMMENTS	
FR. SIGNATURE	
FS. DATE	
FT. APPROVAL	
FU. COMMENTS	
FV. SIGNATURE	
FW. DATE	
FX. APPROVAL	
FY. COMMENTS	
FZ. SIGNATURE	
GA. DATE	
GB. APPROVAL	
GC. COMMENTS	
GD. SIGNATURE	
GE. DATE	
GF. APPROVAL	
GG. COMMENTS	
GH. SIGNATURE	
GI. DATE	
GJ. APPROVAL	
GK. COMMENTS	
GL. SIGNATURE	
GM. DATE	
GN. APPROVAL	
GO. COMMENTS	
GP. SIGNATURE	
GQ. DATE	
GR. APPROVAL	
GS. COMMENTS	
GT. SIGNATURE	
GU. DATE	
GV. APPROVAL	
GW. COMMENTS	
GX. SIGNATURE	
GY. DATE	
GZ. APPROVAL	
HA. COMMENTS	
HB. SIGNATURE	
HC. DATE	
HD. APPROVAL	
HE. COMMENTS	
HF. SIGNATURE	
HG. DATE	
HH. APPROVAL	
HI. COMMENTS	
HJ. SIGNATURE	
HK. DATE	
HL. APPROVAL	
HM. COMMENTS	
HN. SIGNATURE	
HO. DATE	
HP. APPROVAL	
HQ. COMMENTS	
HR. SIGNATURE	
HS. DATE	
HT. APPROVAL	
HU. COMMENTS	
HV. SIGNATURE	
HW. DATE	
HX. APPROVAL	
HY. COMMENTS	
HZ. SIGNATURE	
IA. DATE	
IB. APPROVAL	
IC. COMMENTS	
ID. SIGNATURE	
IE. DATE	
IF. APPROVAL	
IG. COMMENTS	
IH. SIGNATURE	
II. DATE	
IJ. APPROVAL	
IK. COMMENTS	
IL. SIGNATURE	
IM. DATE	
IN. APPROVAL	
IO. COMMENTS	
IP. SIGNATURE	
IQ. DATE	
IR. APPROVAL	
IS. COMMENTS	
IT. SIGNATURE	
IU. DATE	
IV. APPROVAL	
IW. COMMENTS	
IX. SIGNATURE	
IY. DATE	
IZ. APPROVAL	
JA. COMMENTS	
JB. SIGNATURE	
JC. DATE	
JD. APPROVAL	
JE. COMMENTS	
JF. SIGNATURE	
JG. DATE	
JH. APPROVAL	
JI. COMMENTS	
JJ. SIGNATURE	
JK. DATE	
JL. APPROVAL	
JM. COMMENTS	
JN. SIGNATURE	
JO. DATE	
JP. APPROVAL	
JQ. COMMENTS	
JR. SIGNATURE	
JS. DATE	
JT. APPROVAL	
JU. COMMENTS	
JV. SIGNATURE	
JW. DATE	
JX. APPROVAL	
JY. COMMENTS	
JZ. SIGNATURE	
KA. DATE	
KB. APPROVAL	
KC. COMMENTS	
KD. SIGNATURE	
KE. DATE	
KF. APPROVAL	
KG. COMMENTS	
KH. SIGNATURE	
KI. DATE	
KJ. APPROVAL	
KK. COMMENTS	
KL. SIGNATURE	
KM. DATE	
KN. APPROVAL	
KO. COMMENTS	
KP. SIGNATURE	
KQ. DATE	
KR. APPROVAL	
KS. COMMENTS	
KT. SIGNATURE	
KU. DATE	
KV. APPROVAL	
KW. COMMENTS	
KX. SIGNATURE	
KY. DATE	
KZ. APPROVAL	
LA. COMMENTS	
LB. SIGNATURE	
LC. DATE	
LD. APPROVAL	
LE. COMMENTS	
LF. SIGNATURE	
LG. DATE	
LH. APPROVAL	
LI. COMMENTS	
LJ. SIGNATURE	
LK. DATE	
LL. APPROVAL	
LM. COMMENTS	
LN. SIGNATURE	
LO. DATE	
LP. APPROVAL	
LQ. COMMENTS	
LR. SIGNATURE	
LS. DATE	
LT. APPROVAL	
LU. COMMENTS	
LV. SIGNATURE	
LW. DATE	
LX. APPROVAL	
LY. COMMENTS	
LZ. SIGNATURE	
MA. DATE	
MB. APPROVAL	
MC. COMMENTS	
MD. SIGNATURE	
ME. DATE	
MF. APPROVAL	
MG. COMMENTS	
MH. SIGNATURE	
MI. DATE	
MJ. APPROVAL	
MK. COMMENTS	
ML. SIGNATURE	
MM. DATE	
MN. APPROVAL	
MO. COMMENTS	
MP. SIGNATURE	
MQ. DATE	
MR. APPROVAL	
MS. COMMENTS	
MT. SIGNATURE	
MU. DATE	
MV. APPROVAL	
MW. COMMENTS	
MX. SIGNATURE	
MY. DATE	
MZ. APPROVAL	
NA. COMMENTS	
NB. SIGNATURE	
NC. DATE	
ND. APPROVAL	
NE. COMMENTS	
NF. SIGNATURE	
NG. DATE	
NH. APPROVAL	
NI. COMMENTS	
NJ. SIGNATURE	
NK. DATE	
NL. APPROVAL	
NM. COMMENTS	
NN. SIGNATURE	
NO. DATE	
NP. APPROVAL	
NQ. COMMENTS	
NR. SIGNATURE	
NS. DATE	
NT. APPROVAL	
NU. COMMENTS	
NV. SIGNATURE	
NW. DATE	
NX. APPROVAL	
NY. COMMENTS	
NZ. SIGNATURE	
OA. DATE	
OB. APPROVAL	
OC. COMMENTS	
OD. SIGNATURE	
OE. DATE	
OF. APPROVAL	
OG. COMMENTS	
OH. SIGNATURE	
OI. DATE	
OJ. APPROVAL	
OK. COMMENTS	
OL. SIGNATURE	
OM. DATE	
ON. APPROVAL	
OO. COMMENTS	
OP. SIGNATURE	
OQ. DATE	
OR. APPROVAL	
OS. COMMENTS	
OT. SIGNATURE	
OU. DATE	
OV. APPROVAL	
OW. COMMENTS	
OX. SIGNATURE	
OY. DATE	
OZ. APPROVAL	
PA. COMMENTS	
PB. SIGNATURE	
PC. DATE	
PD. APPROVAL	
PE. COMMENTS	
PF. SIGNATURE	
PG. DATE	
PH. APPROVAL	
PI. COMMENTS	
PJ. SIGNATURE	
PK. DATE	
PL. APPROVAL	
PM. COMMENTS	
PN. SIGNATURE	
PO. DATE	
PP. APPROVAL	
PQ. COMMENTS	
PR. SIGNATURE	
PS. DATE	
PT. APPROVAL	
PU. COMMENTS	
PV. SIGNATURE	
PW. DATE	
PX. APPROVAL	
PY. COMMENTS	
PZ. SIGNATURE	
QA. DATE	
QB. APPROVAL	
QC. COMMENTS	
QD. SIGNATURE	
QE. DATE	
QF. APPROVAL	
QG. COMMENTS	
QH. SIGNATURE	
QI. DATE	
QJ. APPROVAL	
QK. COMMENTS	
QL. SIGNATURE	
QM. DATE	
QN. APPROVAL	
QO. COMMENTS	
QP. SIGNATURE	
QQ. DATE	
QR. APPROVAL	
QS. COMMENTS	
QT. SIGNATURE	
QU. DATE	
QV. APPROVAL	
QW. COMMENTS	
QX. SIGNATURE	
QY. DATE	
QZ. APPROVAL	
RA. COMMENTS	
RB. SIGNATURE	
RC. DATE	
RD. APPROVAL	
RE. COMMENTS	
RF. SIGNATURE	
RG. DATE	
RH. APPROVAL	
RI. COMMENTS	
RJ. SIGNATURE	
RK. DATE	
RL. APPROVAL	
RM. COMMENTS	
RN. SIGNATURE	
RO. DATE	
RP. APPROVAL	
RQ. COMMENTS	
RR. SIGNATURE	
RS. DATE	
RT. APPROVAL	
RU. COMMENTS	
RV. SIGNATURE	
RW. DATE	
RX. APPROVAL	
RY. COMMENTS	
RZ. SIGNATURE	
SA. DATE	
SB. APPROVAL	
SC. COMMENTS	
SD. SIGNATURE	
SE. DATE	
SF. APPROVAL	
SG. COMMENTS	
SH. SIGNATURE	
SI. DATE	
SJ. APPROVAL	
SK. COMMENTS	
SL. SIGNATURE	
SM. DATE	
SN. APPROVAL	
SO. COMMENTS	
SP. SIGNATURE	
SQ. DATE	
SR. APPROVAL	
SS. COMMENTS	
ST. SIGNATURE	
SU. DATE	
SV. APPROVAL	
SW. COMMENTS	
SX. SIGNATURE	
SY. DATE	
SZ. APPROVAL	
TA. COMMENTS	
TB. SIGNATURE	
TC. DATE	
TD. APPROVAL	
TE. COMMENTS	
TF. SIGNATURE	
TG. DATE	
TH. APPROVAL	
TI. COMMENTS	
TJ. SIGNATURE	
TK. DATE	
TL. APPROVAL	
TM. COMMENTS	
TN. SIGNATURE	
TO. DATE	
TP. APPROVAL	
TQ. COMMENTS	
TR. SIGNATURE	
TS. DATE	
TT. APPROVAL	
TU. COMMENTS	
TV. SIGNATURE	
TW. DATE	
TX. APPROVAL	
TY. COMMENTS	
TZ. SIGNATURE	
UA. DATE	
UB. APPROVAL	
UC. COMMENTS	
UD. SIGNATURE	
UE. DATE	
UF. APPROVAL	
UG. COMMENTS	
UH. SIGNATURE	
UI. DATE	
UJ. APPROVAL	
UK. COMMENTS	
UL. SIGNATURE	
UM. DATE	
UN. APPROVAL	
UO. COMMENTS	
UP. SIGNATURE	
UQ. DATE	
UR. APPROVAL	
US. COMMENTS	
UT. SIGNATURE	
UU. DATE	
UV. APPROVAL	
UW. COMMENTS	
UX. SIGNATURE	
UY. DATE	
UZ. APPROVAL	
VA. COMMENTS	
VB. SIGNATURE	
VC. DATE	
VD. APPROVAL	
VE. COMMENTS	
VF. SIGNATURE	
VG. DATE	
VH. APPROVAL	
VI. COMMENTS	
VJ. SIGNATURE	
VK. DATE	
VL. APPROVAL	
VM. COMMENTS	
VN. SIGNATURE	
VO. DATE	
VP. APPROVAL	
VQ. COMMENTS	
VR. SIGNATURE	
VS. DATE	
VT. APPROVAL	
VU. COMMENTS	
VV. SIGNATURE	
VW. DATE	
VX. APPROVAL	
VY. COMMENTS	
VZ. SIGNATURE	
WA. DATE	
WB. APPROVAL	
WC. COMMENTS	
WD. SIGNATURE	
WE. DATE	
WF. APPROVAL	
WG. COMMENTS	
WH. SIGNATURE	
WI. DATE	
WJ. APPROVAL	
WK. COMMENTS	
WL. SIGNATURE	
WM. DATE	
WN. APPROVAL	
WO. COMMENTS	
WP. SIGNATURE	
WQ. DATE	
WR. APPROVAL	
WS. COMMENTS	
WT. SIGNATURE	
WU. DATE	
WV. APPROVAL	
WW. COMMENTS	
WX. SIGNATURE	
WY. DATE	
WZ. APPROVAL	
XA. COMMENTS	
XB. SIGNATURE	
XC. DATE	
XD. APPROVAL	
XE. COMMENTS	
XF. SIGNATURE	
XG. DATE	
XH. APPROVAL	
XI. COMMENTS	
XJ. SIGNATURE	
XK. DATE	
XL. APPROVAL	
XM. COMMENTS	
XN. SIGNATURE	
XO. DATE	
XP. APPROVAL	
XQ. COMMENTS	
XR. SIGNATURE	
XS. DATE	
XT. APPROVAL	
XU. COMMENTS	
XV. SIGNATURE	
XW. DATE	
XX. APPROVAL	
XY. COMMENTS	
XZ. SIGNATURE	
YA. DATE	
YB. APPROVAL	
YC. COMMENTS	
YD. SIGNATURE	
YE. DATE	
YF. APPROVAL	
YG. COMMENTS	
YH. SIGNATURE	
YI. DATE	
YJ. APPROVAL	
YK. COMMENTS	
YL. SIGNATURE	
YM. DATE	
YN. APPROVAL	
YO. COMMENTS	
YP. SIGNATURE	
YQ. DATE	
YR. APPROVAL	
YS. COMMENTS	
YT. SIGNATURE	
YU. DATE	
YV. APPROVAL	
YW. COMMENTS	
YX. SIGNATURE	
YY. DATE	
YZ. APPROVAL	
ZA. COMMENTS	
ZB. SIGNATURE	
ZC. DATE	
ZD. APPROVAL	
ZE. COMMENTS	
ZF. SIGNATURE	
ZG. DATE	
ZH. APPROVAL	
ZI. COMMENTS	
ZJ. SIGNATURE	
ZK. DATE	
ZL. APPROVAL	
ZM. COMMENTS	
ZN. SIGNATURE	
ZO. DATE	
ZP. APPROVAL	
ZQ. COMMENTS	
ZR. SIGNATURE	
ZS. DATE	
ZT. APPROVAL	
ZU. COMMENTS	
ZV. SIGNATURE	
ZW. DATE	
ZX. APPROVAL	
ZY. COMMENTS	
ZZ. SIGNATURE	

UNCLASSIFIED

CODING FOR FREQUENCY-HOPPED SPREAD-SPECTRUM

CHANNELS WITH PARTIAL-BAND INTERFERENCE

Wayne Eric Stark, Ph.D.
Department of Electrical Engineering
University of Illinois at Urbana-Champaign, 1982

ABSTRACT

The performance of codes on frequency-hopped spread-spectrum channels with partial-band interference is investigated. The asymptotic performance of codes is measured by the channel capacity and the random coding exponent. The performance of specific codes is measured by the bit error probability. The channel models we consider are quite general and include channels with unknown parameters, channels which change with time, and channels with memory. These models are applicable to frequency-hopped spread-spectrum communication systems as well as to several other communication systems.

We formulate the problem of communicating over channels with unknown transition probabilities (i.e. communicating over channels with jamming) as a game theory problem with payoff function being the mutual information between the channel input and the channel output. Under certain restrictions it is shown that memoryless coding and jamming strategies are simultaneously optimal strategies. Next we develop simple, yet accurate, models for many channels with memory that arise in practice. The channel statistics are constant for blocks of symbols of fixed length. The receiver is said to have side information if it can

determine the channel statistics for each block of symbols transmitted. We determine the capacity, cutoff rate, and random coding exponent for these channels. The capacity without side information is an increasing function of the memory length while the cutoff rate is a decreasing function of the memory length. We show that, for channels with memory and side information random-error correcting codes with interleaving and burst-error correcting codes have comparable performance, while for channels without side information random-error correcting codes with interleaving are inferior to burst-error correcting codes. As a particular example, we examine the performance of several forms of modulation and demodulation with partial-band jamming. Our conclusion is that partial-band jammers can be neutralized provide we use codes with rate less than a constant that depends of the form of modulation and demodulation.

CODING FOR FREQUENCY-HOPPED SPREAD-SPECTRUM
CHANNELS WITH PARTIAL-BAND INTERFERENCE

BY

WAYNE ERIC STARK

B.S., University of Illinois, 1978
M.S., University of Illinois, 1979

THESIS

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Electrical Engineering
in the Graduate College of the
University of Illinois at Urbana-Champaign, 1982

Urbana, Illinois

ACKNOWLEDGEMENT

I would like to thank Professor Robert J. McEliece, my thesis advisor, for his stimulation and encouragement throughout the course of this work. I am also grateful to Professors M. B. Pursley and D. V. Sarwate for many enlightening discussions and to Professor D. V. Sarwate for serving as chairman of the doctoral committee. Thanks are due also to Professor T. Basar for serving on the committee and for proof reading the thesis. Finally, I would like to thank Mrs. Phyllis Young for her speedy and expert typing.

TABLE OF CONTENTS

	Page
CHAPTER 1. INTRODUCTION	1
CHAPTER 2. INFORMATION THEORETIC MODELS.....	7
2.1 Introduction.....	7
2.2 Game Theory Formulation.....	9
2.3 Information Theoretic Interpretation.....	15
2.4 Channels with Memory.....	17
2.5 Channels with Memory and Jamming.....	26
2.6 Performance of Codes on Channels with Memory.....	29
CHAPTER 3. CODING FOR CHANNELS WITH PARTIAL-BAND JAMMING AND COHERENT DEMODULATION.....	35
3.1 Introduction.....	35
3.2 Channel Models.....	35
3.3 Channel Capacity.....	41
3.4 Channel Cutoff Rate.....	55
3.5 Performance of Codes.....	60
CHAPTER 4. CODING FOR CHANNELS WITH PARTIAL-BAND JAMMING AND NONCOHERENT DEMODULATION.....	86
4.1 Introduction.....	86
4.2 Channel Models.....	87
4.3 Channel Capacity.....	90
4.4 Channel Cutoff Rate.....	102
4.5 Performance of Codes.....	109
CHAPTER 5. SUMMARY AND CONCLUSIONS.....	116
APPENDIX A. DERIVATION OF CAPACITY, RANDOM CODING EXPONENT, AND CUTOFF RATE FOR CHANNELS WITH MEMORY.....	118
APPENDIX B. WORST CASE DISTRIBUTION FOR PARTIAL-BAND JAMMING.....	122
APPENDIX C. ERROR PROBABILITY FOR REPETITION CODES ON M-ARY SYMMETRIC CHANNELS.....	126
REFERENCES.....	131
VITA.....	135

CHAPTER 1

INTRODUCTION

In many communication systems the noise present is not entirely due to thermal noise in the receiver. Many communication systems must operate in the presence of interference or noise from other sources. For reliable communication, these systems must be designed to perform acceptably even in the presence of interference. Often very little information is known about the particular form of the interference. It could be that the power of the interfering signal is known or is known to be less than some number but little other information is given on the structure of the interference. For such situations the communication system must be robust to the particular form of the interference.

In many applications there is the possibility that the communication system must operate when there is a hostile source of interference (called a jammer) which tries to make the performance as unreliable as possible. One way to combat this type of hostile interference is through the use of spread-spectrum modulation. If the power of the interference is concentrated in a certain frequency band then if the transmitter uses more bandwidth than is necessary for reliable communication in the presence of thermal noise only, this interference will have less of an effect on the output of the receiver. This is due to the fact that the interference now is occupying a smaller fraction of the frequency band being used by the transmitter-receiver.

There are many forms of spread-spectrum (SS) modulation that can be presently implemented. One form of SS is direct-sequence [11]. Direct-sequence spread-spectrum modulation uses signals with a particular structure in order to minimize the effect of certain types of interference. Another form of

spread-spectrum is frequency-hopped spread spectrum [11],[39]. This form of SS changes its carrier frequency according to a specified hopping pattern and then reverses this operation at the receiver. Only interference at the same frequency of the transmitted signal affects the performance of the system. All other interference is rejected by filters in the frequency dehopper. A third form of spread-spectrum modulation is chirp SS [11],[39]. The idea behind this form of modulation is to continuously change the instantaneous frequency of the signal so that interference at a particular frequency affects the output only a fraction of the time. There are other forms of spread-spectrum modulation. A combination of two or more of the above modulation forms is also possible and should be considered as a possible SS modulation. The different forms of spread-spectrum modulation have different characteristics. One type of SS modulation might yield reliable communication for one type of interference whereas another modulation performs poorly for the same interference.

In this thesis we will consider frequency-hopped (FH) spread-spectrum communications subject to interference that is in only a fraction of the total spread bandwidth the transmitter is using. There are many systems that have this type of interference. The prime example of this is a communication system with a partial-band jammer. This type of jammer concentrates all the available power in only a fraction of the spread bandwidth of the transmitter. Interference in a fraction of the band arises also in a spread-spectrum multiple-access communication system with different users using different hopping patterns. Interference occurs when two users hop to the same frequency at the same time. Yet another situation which gives rise to partial-band interference is when there is some fading of the transmitted signal in certain frequency bands. Then with FH SS modulation we have fading

in certain frequency bands and no fading in other frequency bands. Although we are considering frequency-hopped spread-spectrum modulation the models developed are applicable to other forms of modulation with different interference. For example if we use direct-sequence modulation and the interference is a partial-time jammer (pulsed-jammer) then the models for this type of modulation and interference are exactly the same as frequency-hopped spread-spectrum with partial-band jamming.

The effect of partial-band jamming on the average error probability can be easily determined with frequency-hopped spread-spectrum communications. Consider a jammer that adds noise to the transmitted signal in only a fraction of the frequency band being used. If the total power of the jammer is held fixed, then in a fraction of the band, the noise power density is larger than if the jammer was spreading his power over the entire frequency band. As a result the signal-to-noise ratio in the fraction of the band jammed is reduced by a factor corresponding to the fraction of the band jammed. Since there is no jamming noise in the fraction of the band that is not jammed the signal-to-noise ratio is very large. When the jammer chooses to corrupt the entire frequency band the error probability is typically an exponentially decreasing function of the signal-to-noise ratio. When the jammer chooses the fraction of the band to jam in an optimal way then the probability is an inverse linear function of the average signal-to-noise ratio. The degradation due to intelligent jamming is a severe penalty to be paid in terms of performance (as much as 30-40 dB increase in necessary power for the same error rate). Methods that can reduce the loss due to intelligent jamming must be considered.

For communication systems with intelligent jamming spread-spectrum alone is insufficient to provide adequate performance. In this thesis we prove that indeed this loss can be entirely eliminated by suitable coding techniques combined with spread-spectrum modulation.

There are several key issues that arise when considering coding with spread-spectrum communications in the presence of partial-band interference. One key issue is whether or not the decoder knows if the received signal has been jammed or not. Naturally knowing this side information and using this in a clever way in the decoder can improve the performance compared to coding without side information. Another issue which must be addressed is that of interleaving. The interference in a spread-spectrum communication system may have memory. In this case there are two options with coding: interleave and use random error correcting codes or use burst correcting codes. Previous work in coding has mostly been in evaluating the performance of specific random error correcting codes on these channels [18], [21], [31], [41], [44] or in computing the computational cutoff rate for these channels [2], [4], [8], [42], [43]. All of the papers on coding considered full interleaving to eliminate the channel memory used random error correcting codes. In [7] the degradation due to partial interleaving with random error correcting codes was considered. The papers on the channel cutoff rate have also considered the degradation of partial interleaving when using random error correcting codes.

In this thesis we consider the performance of channels with partial-band interference from several viewpoints. In Chapter 2 we start by considering a game theoretic approach to communication in the presence of interference which henceforth we shall refer to as jamming. The payoff function is taken

to be the mutual information between the input of the channel and the output of the channel. We show that, under certain restrictions on the allowable strategies the jammer and coder may have, the optimal strategies are to be memoryless; i.e. memoryless coding and jamming are the optimal strategies for the coder and jammer. The payoff function is chosen to be the mutual information for the following reason. It can be shown that codes and a decoding rule exist such that reliable communication is possible for any allowable strategy of the jammer provided the code rate is less than the value of the game with mutual information as the payoff function. Although memoryless jamming is optimal, many situations arise in which the jamming signal has memory. A model is presented in Chapter 2 which takes into account the possibility of partial-band jamming and memory. This model is simple enough to be mathematically tractable and yet gives an accurate description of the channel behavior. This model highlights the combined effect of channel memory and side information at the receiver concerning the presence of a jammer. The basic feature of the model is the block nature of the memory. This is perhaps the main feature of frequency-hopped spread-spectrum communication. With FH SS in many cases the interference at different frequencies are statistically independent so that the channel is in fact a memoryless channel from hop to hop. We conclude that when side information is available interleaving does not degrade the performance, but without side information available the channel capacity is decreased with interleaving. Also in Chapter 2 we take a particular example and evaluate the performance of random error correcting codes and burst error correcting codes on channels with and without side information (with full interleaving for the random error correcting code) to verify the conclusions obtained from capacity considerations.

In Chapters 3 and 4 we consider channels with a particular form of demodulation. Chapter 3 treats the case of coherent demodulation and in Chapter 4 noncoherent demodulation is considered. In both chapters we consider the channel capacity, cutoff rate and coded error probability of frequency-hopped spread-spectrum communications in the presence of partial-band jamming. We consider channels with memory with and without side information available. From capacity, cutoff rate and coded error probability we conclude that provided codes with small enough rate are used, the optimal strategy of the jammer is to jam the entire band so that the loss incurred from intelligent jamming is in fact completely recovered by coding with small rates. This is true with and without side information available. Also it is shown that in many cases there exists an optimal code rate that the coder wishes to use in order to minimize the energy needed to transmit any symbol reliably. Various coding schemes are calculated for cases of side information available and interleaving also.

In Chapter 5 we make some comparisons between various coding strategies and draw some conclusions concerning coding for channels with partial-band interference.

CHAPTER 2

INFORMATION THEORETIC MODELS

2.1 Introduction

In this chapter we take an information theoretic viewpoint of frequency-hopped spread-spectrum channels. The models we consider are general enough to include several forms of interference including partial-band jamming, nonselective fading, and multiple access interference. The basic feature of frequency-hopped spread-spectrum communication is the ability of the transmitter to change the frequency of the signal transmitted. The assumption we make in describing the models is that when the frequency changes the interference at the new frequency is independent of the interference at all previous frequencies. The channel accepts symbols from an input alphabet A and produces symbols in an output alphabet B . The input symbols are partitioned into blocks of length n . Each block of n symbols is transmitted at a particular frequency chosen according to a hopping pattern. Since the interference at a particular frequency is independent of the interference at other frequencies two symbols in different blocks are affected by the interference independently. This is not necessarily true for two symbols in the same block of n symbols. Because of this the channel is not memoryless. Consider now the new channel with input alphabet A^n and output alphabet B^n . The new channel has as input symbols a single block of n symbols from the alphabet A . The output symbols are blocks of n symbols from the output alphabet B . Since two blocks of n symbols are transmitted at different frequencies and are affected independently, the new channel is a memoryless channel. We make the following definition for any channel. We say a channel is block n memoryless if the new channel which has

as symbols blocks of n symbols from the original channel is a memoryless channel. Block 1 memoryless is memoryless in the usual sense [27]. It is important to point out that the transmitter knows which n symbols constitute a block and are transmitted at a particular frequency since this will be crucial in the analysis to follow. Thus frequency hopping with n bits per hop and interference which is independent at different frequencies forms a block n memoryless channel.

In this chapter we consider block n memoryless channels from an information theoretic viewpoint. In Section 2.2 we consider a game theory formulation for block n memoryless channels and determine the worst block n memoryless channel and the optimal coding strategy. The game theory approach uses the mutual information between the channel input and output as the payoff function. This is justified in Section 2.3 where we state coding theorems to show existence of codes with rates less than the value of the game and with arbitrarily small error probability. In Section 2.4 we consider a particular type of block n memoryless channels. These channels are block-1 memoryless when conditioned on an external random variable that typically describes the level of noise in a particular block. Capacity, cutoff rate, and the reliability function are determined for these channels. Channels with both memory and jamming are considered in Section 2.5. Finally, in Section 2.6 we consider the performance of specific codes on channels with memory. We consider Reed-Solomon codes which have code symbols as blocks of n symbols. The performance of convolutional codes with interleaving is also determined. We compute the performance of these codes on channel with and without side information at the decoder and conclusions are drawn that coincide with conclusions from capacity considerations.

2.2 Game Theory Formulation

The communication channel we consider has input alphabet A and output alphabet B. Player I called the coder, wishes to communicate information through the channel reliably with largest possible rate. Player II, called the jammer, wants to minimize the rate at which information can be transmitted through the channel. The channel is described by specifying two random variables, X and Y. The random variable X is the input to the channel from the coder and the random variable Y is the output of the channel. The coder's strategies are distributions F_X on the random variable X while the jammer's strategies are the distributions $G_Y(y|a)$ on the output of the channel when $X = a$ is the input. The jammer thus chooses the conditional probabilities of the output given the input while the coder chooses the distribution of the input. We restrict the set of distributions the players can have as follows. The allowable distributions (strategies) for the coder are given by a set S. The collection $\{G_Y(y|a): a \in A\}$, which we denote by $\mathcal{G}_Y$, is required to be in a set T of allowable channels. The payoff function $\phi(F_X, \mathcal{G}_Y)$ for this game is taken to be the mutual information $I(X;Y)$ between the input to the channel X and the output of the channel Y. The objective of player I is to choose $F_X \in S$ to make $\phi(F_X, \mathcal{G}_Y)$ as large as possible. Player II chooses $\mathcal{G}_Y \in T$ to minimize $\phi(F_X, \mathcal{G}_Y)$. Thus associated with the game are two programs:

Program I (Coder's Program)

$$C' = \sup_{F_X \in S} \inf_{\mathcal{G}_Y \in T} \phi(F_X, \mathcal{G}_Y)$$

Program II (Jammer's Program)

$$C'' = \inf_{\mathcal{J}_Y \in T} \sup_{F_X \in S} \phi(F_X, \mathcal{J}_Y) .$$

A strategy $F_X^* \in S$ such that $\inf\{\phi(F_X^*, \mathcal{J}_Y) : \mathcal{J}_Y \in T\} = C'$ is called an optimal strategy for the coder. Similarly if $\sup\{\phi(F_X, \mathcal{J}_Y^*) : F_X \in S\} = C''$ then $\mathcal{J}_Y^*$ is called an optimal strategy for the jammer.

It is clear from the above programs that $C' \leq C''$ and it is easy to give examples where $C' < C''$. However, since ϕ is concave in F_X and convex in $\mathcal{J}_Y$ ([27], Theorems 1.6 and 1.7) if S and T are compact convex sets then $C' = C''$ [38]. This equality is equivalent to the existence of a saddle point i.e. a pair of strategies $F_X^* \in S$, $\mathcal{J}_Y^* \in T$ such that

$$\phi(F_X, \mathcal{J}_Y^*) \leq \phi(F_X^*, \mathcal{J}_Y^*) \leq \phi(F_X^*, \mathcal{J}_Y) \quad \forall F_X \in S, \mathcal{J}_Y \in T . \quad (2.1)$$

If (2.1) holds then F_X^* and $\mathcal{J}_Y^*$ are optimal strategies for the coder and jammer respectively. This game theory formulation was considered by Dobrushin [12] and Blachman [3].

We generalize this game theory formulation by allowing the players to adopt n -dimensional strategies (i.e., non-memoryless strategies). We extend the definition of admissible strategies to higher dimensions by using the notion of the mixture of a set of distribution functions. Let the n dimensional distribution $F_{\underline{X}}^{(n)}(\underline{x})$, $\underline{X} = (X_1, \dots, X_n)$, $\underline{x} = (x_1, x_2, \dots, x_n)$ have marginal distribution $F_{X_i}^{(n)}(x) = F_{\underline{X}}^{(n)}(\infty, \dots, \infty, x, \infty, \dots, \infty)$ with the i -th component being x . We say $F_{\underline{X}}^{(n)} \in S^{(n)}$ if the uniform mixture of the marginals is in S :

$$F_{\underline{X}}^{(n)} \in S^{(n)} \text{ if } \frac{1}{n} \sum_{i=1}^n F_{X_i}^{(n)}(x) \in S . \quad (2.2)$$

The admissible strategies for the jammer are defined similarly. We say

$\mathcal{J}_Y^{(n)} \triangleq \{G_Y^{(n)}(y|\underline{a}) : \underline{a} \in A^n\} \in T^{(n)}$ where $G_Y^{(n)}(y|\underline{a})$ is the n dimensional conditional distribution of the output of the channel given the input $\underline{X} = \underline{a}$, if the uniform mixture of the conditional marginals $G_{Y_i}(y|a)$ is in T :

$$\mathcal{J}_Y^{(n)} \in T^{(n)} \text{ if } \bar{\mathcal{J}}_Y \in T \quad (2.3)$$

where $\bar{\mathcal{J}}_Y = \{G_Y^{(n)}(y|\underline{a}) : \frac{1}{n} \sum_{i=1}^n G_{Y_i}(y|a_i) \in T, \underline{a} \in A^n\}$ is the collection of conditional distributions with uniform mixture of the marginals $G_{Y_i}(y|a)$ in T .

We note here that we have restricted the strategies to those with no "intersymbol interference"; i.e. previous inputs are not allowed to affect current outputs. For these generalized strategies we have the following programs:

Program I_n:

$$C'_n = \sup_{F_X^{(n)} \in S^{(n)}} \inf_{\mathcal{J}_Y^{(n)} \in T^{(n)}} \phi(F_X^{(n)}, \mathcal{J}_Y^{(n)})$$

Program II_n:

$$C''_n = \inf_{\mathcal{J}_Y^{(n)} \in T^{(n)}} \sup_{F_X^{(n)} \in S^{(n)}} \phi(F_X^{(n)}, \mathcal{J}_Y^{(n)})$$

where the payoff function is now $\phi(F_X^{(n)}, \mathcal{J}_Y^{(n)}) = \frac{1}{n} I(\underline{X}; \underline{Y})$. We have the following result concerning C'_n and C''_n .

Theorem 1: $C'_n = C'$ and $C''_n = C''$ for all $n \geq 1$.

Proof: First we prove $C'_n = C'$. Let F_X be an admissible strategy i.e.

$F_X \in S$ and let $\mathcal{J}_Y^{(n)} \in T^{(n)}$ be an admissible strategy for the jammer. Then if $\underline{X} = (X_1, X_2, \dots, X_n)$ is a random vector consisting of n independent identically distributed (i.i.d.) copies of X we have

$$\phi(F_{\underline{X}}^{(n)}, \mathcal{G}_{\underline{Y}}^{(n)}) \geq \frac{1}{n} \sum_{i=1}^n \phi(F_{\underline{X}}, \mathcal{G}_{Y_i}) \quad ([27], \text{Theorem 1.8})$$

$$\geq \phi(F_{\underline{X}}, \bar{\mathcal{G}}_{\underline{Y}}) \quad ([27], \text{Theorem 1.7})$$

where $\bar{\mathcal{G}}_{\underline{Y}}$ is the collection of uniform mixtures of the conditional distributions G_{Y_i} . Since $\bar{\mathcal{G}}_{\underline{Y}} \in T^{(n)}$ we have

$$\mathcal{G}_{\underline{Y}}^{(n)} \inf_{T^{(n)}} \phi(F_{\underline{X}}^{(n)}, \mathcal{G}_{\underline{Y}}^{(n)}) \geq \inf_{\mathcal{G}_{\underline{Y}} \in T} \phi(F_{\underline{X}}, \mathcal{G}_{\underline{Y}})$$

$$F_{\underline{X}}^{(n)} \sup_{S^{(n)}} \mathcal{G}_{\underline{Y}}^{(n)} \inf_{T^{(n)}} \phi(F_{\underline{X}}^{(n)}, \mathcal{G}_{\underline{Y}}^{(n)}) \geq \sup_{F_{\underline{X}} \in S} \inf_{\mathcal{G}_{\underline{Y}} \in T} \phi(F_{\underline{X}}, \mathcal{G}_{\underline{Y}})$$

so that $C'_n \geq C'$. Now let $F_{\underline{X}}^{(n)} \in S^{(n)}$ and $G_Y(y|a)$ be arbitrary. Then if $G_{\underline{Y}}^{(n)}$ is the n -dimensional distribution of $\underline{Y} = (Y_1, \dots, Y_n)$ given $\underline{X} = \underline{a}$ with Y_i conditionally independent then

$$\phi(F_{\underline{X}}^{(n)}, \mathcal{G}_{\underline{Y}}^{(n)}) \leq \frac{1}{n} \sum_{i=1}^n \phi(F_{\underline{X}_i}, \mathcal{G}_{Y_i}) \quad ([27], \text{Theorem 1.9})$$

$$\leq \phi(F_{\underline{X}}, \mathcal{G}_{\underline{Y}}) \quad ([27], \text{Theorem 1.6})$$

where $F_{\underline{X}}$ is the uniform mixture of $F_{\underline{X}}^{(n)}$; i.e. $F_{\underline{X}}(x) = \frac{1}{n} \sum_{i=1}^n F_{\underline{X}_i}(x)$.

Since $F_{\underline{X}} \in S$ we have

$$\mathcal{G}_{\underline{Y}}^{(n)} \inf_{T^{(n)}} \phi(F_{\underline{X}}^{(n)}, \mathcal{G}_{\underline{Y}}^{(n)}) \leq \inf_{\mathcal{G}_{\underline{Y}} \in T} \phi(F_{\underline{X}}, \mathcal{G}_{\underline{Y}})$$

$$F_{\underline{X}}^{(n)} \sup_{S^{(n)}} \mathcal{G}_{\underline{Y}}^{(n)} \inf_{T^{(n)}} \phi(F_{\underline{X}}^{(n)}, \mathcal{G}_{\underline{Y}}^{(n)}) \leq \sup_{F_{\underline{X}} \in S} \inf_{\mathcal{G}_{\underline{Y}} \in T} \phi(F_{\underline{X}}, \mathcal{G}_{\underline{Y}})$$

so that $C'_n \leq C'$. Thus $C'_n = C'$ as asserted. Similarly $C''_n = C''$.

What we have shown is that of all block n memoryless channels, the channel with minimum mutual information is the block 1 memoryless channel.

The conclusions one can draw from this are that memoryless jamming is

optimal $(G_Y^{(n)*}(\underline{y}|\underline{x}) = \prod_{i=1}^n G^*(y_i|x_i))$ and memoryless coding is optimal

$(F_X^{(n)*}(\underline{x}) = \prod_{i=1}^n (F_{X_i}^*(x_i)))$. Thus, of all types of interference, the one that minimizes the mutual information is independent from symbol to symbol.

As an example let $A = B = \{0, 1, \dots, M-1\}$ and let T be the set of channels with error probability per symbol less than ϵ , $0 \leq \epsilon \leq 1$ and S be all distributions on A . Then a result of Dobrushin [12] is that

$$C' = C'' = \begin{cases} \log M + (1-\epsilon)\log(1-\epsilon) + \epsilon \log \epsilon - \epsilon \log(M-1), & \epsilon \leq 1 - \frac{1}{M} \\ 0, & \epsilon \geq 1 - \frac{1}{M} \end{cases} \quad (2.4)$$

Here C' and C'' are measured in bits per channel use and all logarithms have base 2. The optimal distribution $F_X^*(x)$ is the uniform distribution on $\{0, 1, \dots, M-1\}$ and the optimal channel $G^*(y|x)$ satisfies

$$G^*(y|x) = \begin{cases} \epsilon/(M-1), & y \neq x, \quad \epsilon \leq 1 - \frac{1}{M} \\ 1 - \epsilon, & y = x, \quad \epsilon \leq 1 - \frac{1}{M} \\ \frac{1}{M}, & \epsilon \geq 1 - \frac{1}{M} \end{cases} \quad (2.5)$$

Here we generalize this game to the n dimensional case and apply the theorem.

For the generalized strategies we use the channel n times to transmit n

symbols. Let ϵ_i be the error probability of the i -th channel. Then $T^{(n)}$ is the set of channels with $\frac{1}{n} \sum_{i=1}^n \epsilon_i \leq \epsilon$. Also $S^{(n)}$ is the set of

distributions on A^n . By the Theorem 1 $C'_n = C'$ and $C''_n = C'$ and is given in (2.4). The optimal strategies are memoryless with marginals $F_X^*(x)$ and $G_Y^*(y|x)$ given above. A conclusion one can draw is that if the average error probability is less than ϵ then with memoryless encoding $I(\underline{X}; \underline{Y}) \geq C' = C''$ with equality for the optimal strategy given above.

As a second example consider $A = B = \mathbb{R}$, the real line. Let

$$S = \{F_X(x): \int_{\mathbb{R}} x^2 dF_X(x) \leq E\} \quad (2.6)$$

and

$$T = \{G_Y(y|x): \int_{y \in \mathbb{R}} (y-x)^2 dG_Y(y|x) \leq N, x \in A\}. \quad (2.7)$$

The set of channels is restricted to channels whose added noise has mean square less than or equal to N . For S and T given in (2.6) and (2.7) a result of Dobrushin [12] and Blachman [3] shows that

$$C' = C'' = \frac{1}{2} \log(1 + \frac{E}{N}) \quad (2.8)$$

with $F^*(x) = \Phi(x/\sqrt{E})$ and $G_Y^*(y|x) = \Phi(\frac{y-x}{\sqrt{N}})$ where $\Phi(u)$ is given by

$$\Phi(u) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^u e^{-x^2/2} dx \quad (2.9)$$

Again we generalize this game to allow for n dimensional distributions.

The set $S^{(n)}$ and $T^{(n)}$ are given by

$$S^{(n)} = \{F_{\underline{X}}^{(n)}(\underline{x}): \frac{1}{n} \int_{\mathbb{R}^n} \underline{x} \cdot \underline{x}' dF_{\underline{X}}^{(n)}(\underline{x}) \leq E\}$$

where $\underline{x}'$ denotes the transpose of the vector $\underline{x}$. Similarly

$$T^{(n)} = \{G_Y^{(n)}(Y|X) : \frac{1}{n} \int_{Y \in \mathbb{R}^n} (Y-X)(Y-X)' dG_Y^{(n)}(Y|X) \leq N, X \in A^n\}.$$

By Theorem 1 $C'_n = C''_n = C' = C''$ and the optimal distributions are memoryless with marginal distributions being Gaussian.

2.3 Information Theoretic Interpretation

In this section we give an information theoretic interpretation to the results of the previous sections. We consider the existence of codes which achieve reliable communication for all strategies the jammer or nature can present to the coder. Here we state the results that apply from the literature to our particular problem. First we clarify the model we are considering. Then some definitions are necessary in order to state the results.

First we are going to consider only memoryless channels since block n memoryless channels are memoryless channels with larger alphabet sizes. There are essentially two different methods a jammer might choose a channel from the restricted set T in order to minimize the performance. One way, which results in a channel called the compound channel [46], is for the jammer to choose a channel from T and force the coder to use this channel for every symbol transmitted in a codeword. The other way is for the jammer to choose an element in T for each symbol transmitted. The channel then might change from symbol to symbol of a codeword. This is called an arbitrarily varying channel (AVC) [46]. Below we state some results on the existence of codes for these channels. A code (n, M, λ) is defined as a set $\{(u_1, B_1), (u_2, B_2), \dots, (u_M, B_M)\}$ where u_i , $i = 1, 2, \dots, M$ is a length n

sequence of symbols, with each symbol in A and B_i , $i = 1, 2, \dots, M$ are disjoint sets of length n sequences with elements in B ($B_i \subseteq B^n$, $i = 1, 2, \dots, M$) such that

$$P_{\mathcal{J}}(B_i^c | u_i) \leq \lambda \text{ for } i = 1, 2, \dots, M \text{ and all } \mathcal{J} \in T \quad (2.10)$$

where $u_i = (u_{i1}, u_{i2}, \dots, u_{in})$ and

$$P_{\mathcal{J}}(B_i^c | u_i) = \sum_{y \notin B_i} \prod_{j=1}^n G_{Y_j}(y_j | u_{ij}). \quad (2.11)$$

The rate R of an (n, M, λ) code is $R = \log M/n$. The coding theorem and its converse for compound channels with A and B finite are as follows.

Theorem 2 (Wolfowitz [46]): Let $0 < \lambda \leq 1$ be arbitrary. Then there exists a positive constant K_0 independent of $\mathcal{J}$ such that, for any n , there exists a (n, M, λ) code for T with rate R satisfying

$$R > C' - K_0/\sqrt{n}.$$

Theorem 3 (Wolfowitz [46]): Let $0 < \lambda \leq 1$ be arbitrary. Then there exists a positive constant K'_0 independent of $\mathcal{J}$ such that, for any n , there does not exist a (n, M, λ) code for T with rate R satisfying

$$R = C' + K'_0/\sqrt{n}.$$

The above theorems do not assume the sender (transmitter) or receiver know which channel the jammer has selected for the codeword. If the sender knows which channel the jammer has selected then the above theorems are valid with C' replaced by C'' . If the receiver knows which channel the jammer has selected then the theorems are valid as stated.

The above theorems are stated for the case of finite alphabets. When just the output alphabet is infinite and the input alphabet is finite Theorems 2 and 3 are no longer valid (see [17]). For the case of infinite output alphabet Theorem 2 is valid if we replace C' by $\hat{C}'$ where

$$\hat{C}' = \sup_{F_X \in \mathcal{S}} \sup_P \inf_{J_Y \in \mathcal{T}} I(X, [Y]_P), \quad (2.12)$$

P is a partition of the output alphabet, and $[Y]_P$ is the quantization of Y by P (see [27] p. 34). If however, the receiver knows which channel the jammer selected then Theorems 2 and 3 are valid as stated. The above results for the semicontinuous case were proved by Kesten [17]. Note that in the semicontinuous case $\hat{C}' \leq C'$ so that C' is an upper bound on $\hat{C}'$. In the sequel we will consider C' as the performance measure of the channel, since it is easier to compute than $\hat{C}'$.

Consider now the second method the jammer might use to choose the channel for use by the coder. If the jammer chooses an element of $\mathcal{T}$ for each symbol of a codeword transmitted then we have an arbitrary varying channel. The coding theorems for this case are far less complete than for the compound channel. If the output alphabet B consists of only two letters then Theorems 2 and 3 are valid for the AVC ([46] Section 6.4). For larger output alphabets, see [10] for related results.

2.4 Channels with Memory

In this section we introduce a class of block m memoryless channels that are not block 1 memoryless. These channels are of interest because they model frequency-hopped spread-spectrum channels. After describing the channel models, we derive expressions for the capacity, cutoff rate, and reliability function for these channels.

Let $\{\Delta_s\}$, $s \in \Omega$ denote a collection of memoryless channels, each with input alphabet A and output alphabet B . The index parameter s lies in a set Ω on which a probability distribution P is defined. Let $S_1, S_2, \dots$ be a sequence of independent identically distributed Ω valued random variables,

the common distribution being P . For each integer $m \geq 1$ we define the channels $\Delta(m)$ and $\bar{\Delta}(m)$ with input alphabet A as follows. When a sequence of letters $x_0, x_1, \dots$ from A is transmitted, the k -th block of m consecutive letters, $[x_{(k-1)m}, x_{(k-1)m+1}, \dots, x_{km-1}]$ is in fact transmitted over one of the component channels Δ_s ; the random variable S_k determining which component channel is used. If the receiver gets no direct information concerning which channel was used for the transmission of the k -th block then we call this the channel $\Delta(m)$ without side information. If with each noisy block of m symbols the receiver knows the index s of the component channel being used to transmit that block then we call this the channel $\bar{\Delta}(m)$ with side information. We assume the transmitter can synchronize to the channel in the sense that the transmitter knows which are the first and last letters in the k -th block of m letters. One further assumption is that the receiver knows both the distribution P and the transition probabilities of the component channels. This last assumption will be relaxed slightly in the next section.

Since the channel with (without) side information can be considered as a memoryless channel with input alphabet A^m and output alphabet $B^m \times \Omega$ (B^m), the capacity is found by maximizing the mutual information of the memoryless channel over all input distributions. For the channel without side information we maximize the mutual information $I(\underline{X}; \underline{Y})$ between the vectors $\underline{X} = (X_1, X_2, \dots, X_m)$ and $\underline{Y} = (Y_1, Y_2, \dots, Y_m)$ where

$$I(\underline{X}; \underline{Y}) = E \left\{ \log_2 \left[\frac{p(\underline{Y}|\underline{X})}{p(\underline{Y})} \right] \right\}, \quad (2.13)$$

$$p(\underline{y}|\underline{x}) = E \{p_S(\underline{y}|\underline{x})\} = E \left\{ \prod_{i=1}^n p_S(y_i|x_i) \right\} \quad (2.14)$$

and $p_s(\cdot|\cdot)$ is the transition probability for the component channel Δ_s . The expectation in (2.13) is with respect to the random vectors $\underline{X}$ and $\underline{Y}$ and the expectation in (2.14) is with respect to the random variable S with distribution P . Also in (2.13) $p(\underline{y})$ is the unconditional distribution on the channel output $\underline{Y}$. For the channel with side information the output now consists of $\underline{Y}$ and S . The mutual information $I(\underline{X};\underline{Y},S)$ is given by

$$I(\underline{X};\underline{Y},S) = E \left\{ \log_2 \frac{p_S(\underline{Y}|\underline{X})}{p_S(\underline{Y})} \right\} \quad (2.15)$$

where $p_S(\underline{y})$ is the distribution of the output conditioned only on the random variable S .

The capacity $C(m)$ for the channel without side information measured on a per channel use basis is just

$$C(m) = \max_{\underline{X}} \left\{ \frac{1}{m} I(\underline{X};\underline{Y}) \right\} . \quad (2.16)$$

For the channel with side information the capacity $\bar{C}(m)$ is given by

$$\bar{C}(m) = \max_{\underline{X}} \left\{ \frac{1}{m} I(\underline{X};\underline{Y},S) \right\} . \quad (2.17)$$

In (2.16) and (2.17) the maximization is over all distributions on the random vector $\underline{X}$. If the input distribution that achieves capacity (maximizes mutual information) for each component channel are identical, then $\bar{C}(m)$ is in fact independent of m ($\bar{C} = \bar{C}(m)$) and is just the average of the capacities of the component channels [29]:

$$\bar{C} = E\{C_s\} \quad (2.18)$$

where C_s is the capacity of component channel Δ_s . Furthermore it can be shown that [29]

$$C(m) \leq \bar{C} \quad , \quad (2.19)$$

and if A and B are finite then

$$\lim_{m \rightarrow \infty} C(m) = \bar{C} \quad . \quad (2.20)$$

As an example let $\Omega = [0,1]$ and $\{\Delta_s\}$ be the set of binary symmetric channels with crossover probability s . For this example $A = B = \{0,1\}$. Let $d(\underline{x}, \underline{y})$ denote the Hamming distance between the vectors $\underline{x} = (x_1, x_2, \dots, x_m)$ and $\underline{y} = (y_1, y_2, \dots, y_m)$. The transition probabilities in (2.14) then are easily shown to be

$$\alpha_{m,k} \triangleq P(\underline{y}|\underline{x}) = E\{S^k(1-S)^{m-k}\}, \quad d(\underline{x}, \underline{y}) = k, \quad k = 1, 2, \dots, m. \quad (2.21)$$

The mutual information for the channel $\Delta(m)$ without side information, is maximized by letting X have the uniform distribution (i.e. $P\{X=0\} = P\{X=1\} = \frac{1}{2}$) with $\{X_i\}_{i=1}^m$ independent and identically distributed. The capacity $C(m)$ is thus given by (see Appendix A)

$$C(m) = \max_{\underline{X}} \left\{ \frac{1}{m} I(\underline{X}; \underline{Y}) \right\} = 1 + \frac{1}{m} \sum_{k=0}^m \binom{m}{k} \alpha_{m,k} \log_2 \alpha_{m,k} \quad . \quad (2.22)$$

The factor of m^{-1} in (2.17) is due to the fact that we are measuring the capacity in bits per channel use. The mutual information for the channel $\bar{\Delta}(m)$ with side information is maximized by the same distribution and the capacity $\bar{C}(m)$ is given by

$$\bar{C}(m) = \max_{\underline{X}} \left\{ \frac{1}{m} I(\underline{X}; \underline{Y}, S) \right\} = E\{1 - H_2(S)\} \quad (2.23)$$

where

$$H_2(s) = -s \log_2 s - (1-s) \log_2 (1-s) \quad (2.24)$$

We now consider the random coding exponent $E_r(R)$ for these channels. In order to be consistent with well established notations we change slightly our notation. Let $Q(x)$ be the distribution on the input X to the channel and $p(\underline{y}|\underline{x})$ the distribution on the output vector $\underline{y}$ given the input vector $\underline{x}$ as before. The random coding exponent $E_r(R)$ is defined as

$$E_r(R) = \max_{0 \leq \rho \leq 1} \max_Q [E_0(\rho, Q) - \rho R] \quad (2.25)$$

where

$$E_0(\rho, Q) = -\log_2 \sum_{\underline{y} \in B} \left[\sum_{\underline{x} \in A} Q(\underline{x}) p(\underline{y}|\underline{x})^{1/(1+\rho)} \right]^{1+\rho} \quad (2.26)$$

This function is of interest because of the following result of Gallager:

Theorem 4 (Gallager [13]): There exists an (n, M, λ) code with error probability λ defined in (2.10) satisfying

$$\lambda \leq 4 \cdot 2^{-n E_r(R)} \quad (2.27)$$

where $R = \log_2 M/n$. Furthermore $E_r(R)$ is a convex, decreasing, positive function of R for $0 \leq R < C$, where C is the capacity of the channel.

For block m memoryless channels (2.25) and (2.26) are valid if x and y are replaced by $\underline{x}$ and $\underline{y}$, A and B by A^m and B^m , and $E_o(\rho, Q)$ is normalized by the factor $1/m$. Of special interest is the cutoff rate which is defined as

$$R_0 \triangleq \max_Q E_o(1, Q)$$

which many believe is the largest rate at which practical coding systems can be implemented. The cutoff rate for the channels considered here can be computed as follows. Let $R_{0,s}$ denote the cutoff rate for component channel Δ_s ; $R_0(m)$ the cutoff rate for the channel $\Delta(m)$ and $\bar{R}_0(m)$ the cutoff rate for the channel $\bar{\Delta}(m)$. We can express $\bar{R}_0(m)$ in terms of $R_{0,s}$ as [29]

$$\bar{R}_0(m) = -\frac{1}{m} \log_2 E\{2^{-m R_{0,s}}\} \leq E\{R_{0,s}\} \quad (2.28)$$

The cutoff rate without side information is, in general, less than the cutoff rate with side information:

$$R_0(m) \leq \bar{R}_0(m) \quad .$$

From (2.18) we see that the capacity with side information is independent of m . However, the cutoff rate with side information depends on m and, in all cases considered, decreases as m increases [29], [43]. The cutoff rate without side information is also a decreasing function of m for all cases considered. This is contrary to the increase in capacity with increasing memory length. The limiting value of $\bar{R}_0(m)$ as m becomes large is given by [29]

$$\lim_{m \rightarrow \infty} \bar{R}_0(m) = \text{ess. inf}\{R_{0,s}\}$$

which for the case of finite number of channels with each having positive probability is given by

$$\lim_{m \rightarrow \infty} \bar{R}_0(m) = \min_{s \in \mathcal{S}} R_{0,s} \quad .$$

The function $E_0(\rho, Q)$ for the channels of the previous example can be calculated. We consider only those channels which are symmetric enough so that the maximizing $Q(\underline{x})$ in (2.25), denoted by $Q^*(\underline{x})$, is a constant independent of $\underline{x}$. Using $Q^*(\underline{x}) = 2^{-m}$ and $p(y|\underline{x})$ given in (2.21) we obtain $E_0(\rho, Q^*)$ for the channel without side information as (see Appendix A)

$$E_0(\rho, Q^*) = \rho - \left(\frac{1+\rho}{m} \right) \log_2 \left\{ \sum_{k=0}^m \binom{m}{k} \alpha_{m,k}^{\frac{1}{1+\rho}} \right\} \quad (2.29)$$

with $\alpha_{m,k}$ given in (2.21). For the channel with side information we obtain

$$\bar{E}_0(\rho, Q^*) = \rho - \frac{1}{m} \log_2 E \left(\sum_{k=0}^m \binom{m}{k} \left[s^k (1-s)^{m-k} \right]^{1/(1+\rho)} \right)^{1+\rho} \quad (2.30)$$

where the expectation is with respect to the random variable S with distribution P .

The cutoff rate R_0 for any discrete memoryless channel is found by maximizing the function $E_0(1, Q)$ over all input distributions Q . For the channel without side information the cutoff rate R_0 (assuming $Q^*(\underline{x}) = 2^{-m}$) is given by (see Appendix A)

$$R_0 = 1 - \frac{2}{m} \log_2 \left\{ \sum_{k=0}^m \binom{m}{k} \alpha_{m,k}^{\frac{1}{2}} \right\} \quad (2.31)$$

For the channel with side information the cutoff rate $\bar{R}_0$ is given by

$$\bar{R}_0 = 1 - \frac{1}{m} \log_2 \left\{ \sum_{k=0}^m \sum_{\ell=0}^m \binom{m}{k} \binom{m}{\ell} \alpha_{m, \frac{k+\ell}{2}} \right\} \quad (2.32)$$

The cutoff rate is the intercept of the random coding exponent $E_r(R)$ with the $R = 0$ axis and is the largest linear error exponent. Over a range of rates $R_{cr} \leq R < C$, with R_{cr} a constant, the exponent in the bound is the largest possible. Over this range of rates the random coding exponent is equal to the reliability function defined in Gallager ([13], Eq. 5.8.8).

Let us now consider a specific example of these channels. Let $\Omega = [0, \frac{1}{2}]$, $P[S = 0] = 1 - \epsilon$, $P[S = \frac{1}{2}] = \epsilon$ and $A = B = \{0, 1\}$. Let Δ_0 be a noiseless channel and $\Delta_{\frac{1}{2}}$ be a useless channel (error probability $\frac{1}{2}$). Then $\alpha_{m,k}$ for the channel without side information is given by

$$\alpha_{m,k} = \begin{cases} \epsilon 2^{-m} + 1 - \epsilon, & k = 0 \\ \epsilon 2^{-m}, & k = 1, 2, \dots, m \end{cases} \quad (2.33)$$

Using (2.31) in (2.28) and then (2.28) in (2.25) yields the random coding exponent for this channel. This is plotted in Figure 2.1 for various values of m .

The value of R in Figure 2.1 such that $E_r(R) = 0$ is the capacity C of the channel and the $R = 0$ axis intercept is the cutoff rate R_0 . Note that as m increases the capacity increases so that for rates sufficiently large, channels with larger memory have larger random coding exponents. However, for smaller rates this is no longer true and channels with smaller memory may have larger coding exponents.

Consider now the channel with side information. The random coding exponent $\bar{E}_0(p, Q^*)$ may be calculated as

$$\bar{E}_0(p, Q^*) = p - \frac{1}{m} \log_2 [1 - \epsilon + \epsilon 2^{mc}] \quad (2.34)$$

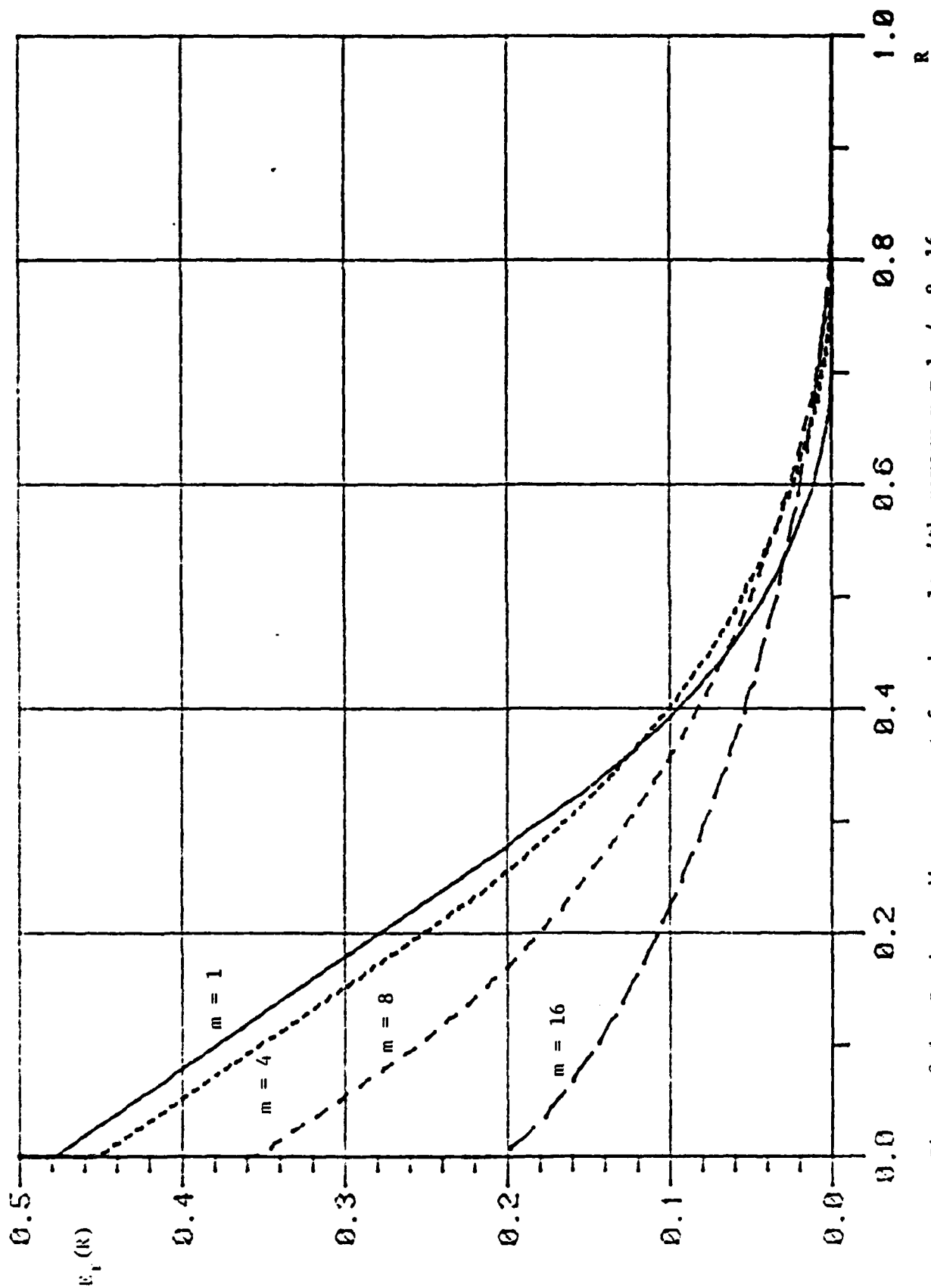


Figure 2.1. Random coding exponent for channels with memory $m = 1, 4, 8, 16$, no side information available and $\epsilon = 0.1$.

This is used in (2.25) to determine the random coding exponent and is plotted in Figure 2.2. Note that the horizontal intercept (the capacity) is independent of m and that at all rates less than capacity, the random coding exponent is larger for channels with smaller memory.

2.5 Channels with Memory and Jamming

In this section we combine the models of channels with memory of the previous section with the models of channels with jamming of Section 2.1 and 2.2 to model frequency hopped channels with non memoryless jamming. The channels with memory of Section 2.3 implicitly assume the receiver knows the distribution P on the component channels and the transition probabilities of each component channel. In this section we consider the case of the jammer choosing both the distribution P and the component channels for some set of allowable distributions and allowable component channels.

Consider a class T of channels with memory. Each channel in the class has the structure of the channels of the previous section being block m memoryless but not block l memoryless. The jammer chooses from the set T a channel for the encoder and decoder to communicate through. Assume that the jammer chooses the channel for each codeword so that we are considering the compound channel model. Then, since we are assuming block memoryless channels, the capacity C' is the same as given in Program I of Section 2.1 with $\phi(F_x, \mathcal{B}_x)$ given by $\frac{1}{m} I(\underline{X}; \underline{Y})$ for the channel without side information and $\frac{1}{m} I(\underline{X}; \underline{Y}, S)$ for the channel with side information. The fact that C' is the capacity is justified by Theorems 2 and 3 for the case of A , B , Ω finite. If B or Ω is infinite then C' is the capacity provided the receiver knows which channel in T the jammer selected.

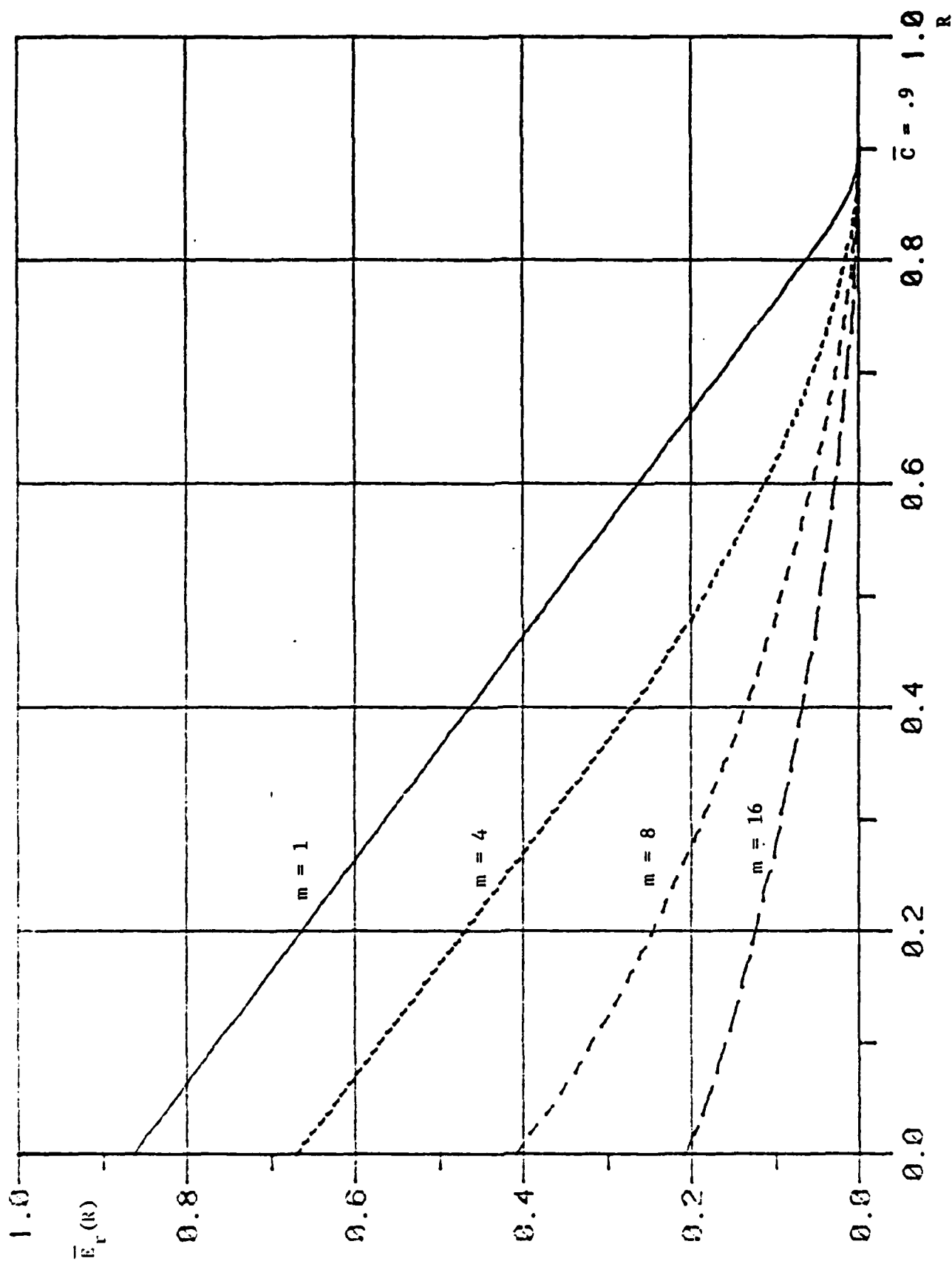


Figure 2.2. Random coding exponent for channels with memory $m = 1, 4, 8, 16$, side information available and $\epsilon = 0.1$.

As an example consider the case $A = B = \{0,1\}$ and $\Omega = \{0,1\}$. Let $P\{S = 1\} = \epsilon$, $P\{S = 0\} = 1 - \epsilon$, Δ_0 be a noiseless binary channel and Δ_1 a binary symmetric channel with crossover probability of $f(\epsilon)$ for some decreasing function f . Then for each $\epsilon \in [0,1]$ we have a different channel. The jammer chooses ϵ and thus the channel for communication.

The capacity C' of this channel when no side information is available is given by

$$C' = \min_{0 \leq \epsilon \leq 1} \left\{ \frac{1}{m} I(\underline{X}; \underline{Y}) \right\} = \min_{0 \leq \epsilon \leq 1} \left\{ 1 + \frac{1}{m} \sum_{k=0}^m \binom{m}{k} \alpha_{m,k} \log_2 \alpha_{m,k} \right\} \quad (2.35)$$

where

$$\alpha_{m,k} = \begin{cases} 1 - \epsilon + \epsilon(1-f(\epsilon))^m & k = 0 \\ \epsilon f^k(\epsilon)(1-f(\epsilon))^{m-k} & k = 1, 2, \dots, m \end{cases} \quad (2.36)$$

When side information is available then the capacity $\bar{C}'$ is given by

$$\bar{C}' = \min_{0 \leq \epsilon \leq 1} \left\{ (1 - \epsilon) + \epsilon \cdot (1 - H_2(f(\epsilon))) \right\} \quad (2.37)$$

We will see in Chapters 3 and 4 that this example is directly applicable to frequency-hopped channels with partial band jamming.

2.6 Performance of Codes on Channels with Memory

Up till now we have only considered asymptotic measures of the channel's ability to convey information. Here we compute the performance of specific codes on a particular channel with memory. We defer the performance of codes on channels with jamming and memory until later. The channel model we consider is that of Section 2.3 with $\Omega = \{0, \frac{1}{2}\}$, $P\{S=0\} = 1 - \epsilon$, $P\{S=\frac{1}{2}\} = \epsilon$, $A = B = \{0,1\}$. Let Δ_0 be a noiseless binary channel and $\Delta_{\frac{1}{2}}$ a binary symmetric channel (BSC) with error probability $\frac{1}{2}$. For this channel we consider Reed-Solomon (RS) codes and convolutional codes with interleaving. We also consider the cases of side information available and not available.

First consider the case of side information available so that the decoder knows which channel each block of m bits was transmitted over. Since the error probability is $\frac{1}{2}$ on channel $\Delta_{\frac{1}{2}}$ the decoder can erase all bits in every block of m bits transmitted over $\Delta_{\frac{1}{2}}$. For R-S codes we treat a block of m bits as one symbol (in $GF(2^m)$) of the code. The probability of a received symbol being erased is just ϵ . For R-S codes the probability of a decoded symbol being in error $P_{e,s}$ for a bounded distance decoder can be computed as [1]

$$P_{e,s} = \sum_{j=n-k+1}^n \frac{j}{n} \binom{n}{j} \epsilon^j (1-\epsilon)^{n-j} . \quad (2.38)$$

If there are more than $n-k$ erasures the R-S code is unable to recover the erased symbols. If the decoder is unable to recover the erased positions the decoder guesses the erased symbols. The bit error probability $P_{e,b}$ is given by

$$P_{e,b} = \frac{1}{2} P_{e,s} . \quad (2.39)$$

We have plotted in Figure 2.3 the bit error probability for two different R-S codes of rate approximately $\frac{1}{2}$. The first is the (255,127) R-S code with symbols in $GF(2^8)$. We consider using this code on $\bar{\Delta}(8)$ (i.e. $m = 8$). The other R-S code is the (31,15) code with rate approximately $\frac{1}{2}$. This code is used on the channel $\bar{\Delta}(5)$ and has symbols in $GF(2^5)$. (We have plotted these versus $10 \log_{10}(1/\epsilon)$ since for partial-band or pulsed jamming the fraction of the band jammed or duty factor is typically inversely proportional to the signal-to-jamming noise ratio.)

The performance of convolutional codes on channel $\bar{\Delta}(m)$ is considered next. Here we consider only binary convolutional codes with interleaving. The viewpoint we take is that interleaving changes channel $\bar{\Delta}(m)$ into channel $\bar{\Delta}(1)$. This can be done by having m convolutional encoders and decoders. Each bit in a block of m bits that is transmitted comes from a different encoder and is decoded by a separate decoder. With this interleaving we have the channel $\bar{\Delta}(1)$ which is just a binary erasure channel with erasure probability ϵ . The bit error probability $P_{e,b}$ for rate k/n convolutional codes with Viterbi decoding is bounded by ([9] Eq. (6-11))

$$P_{e,b} < \frac{1}{k} \sum_{j=d_f}^{\infty} w_j P_j \quad (2.40)$$

where d_f is the free distance of the code, w_j is the total information weight of all paths of weight j , and P_j is the error probability between two words differing in j symbols. For the binary erasure channel P_j is just $\frac{1}{2} \epsilon^j$ since for an error to occur all j symbols must be erased and given that all

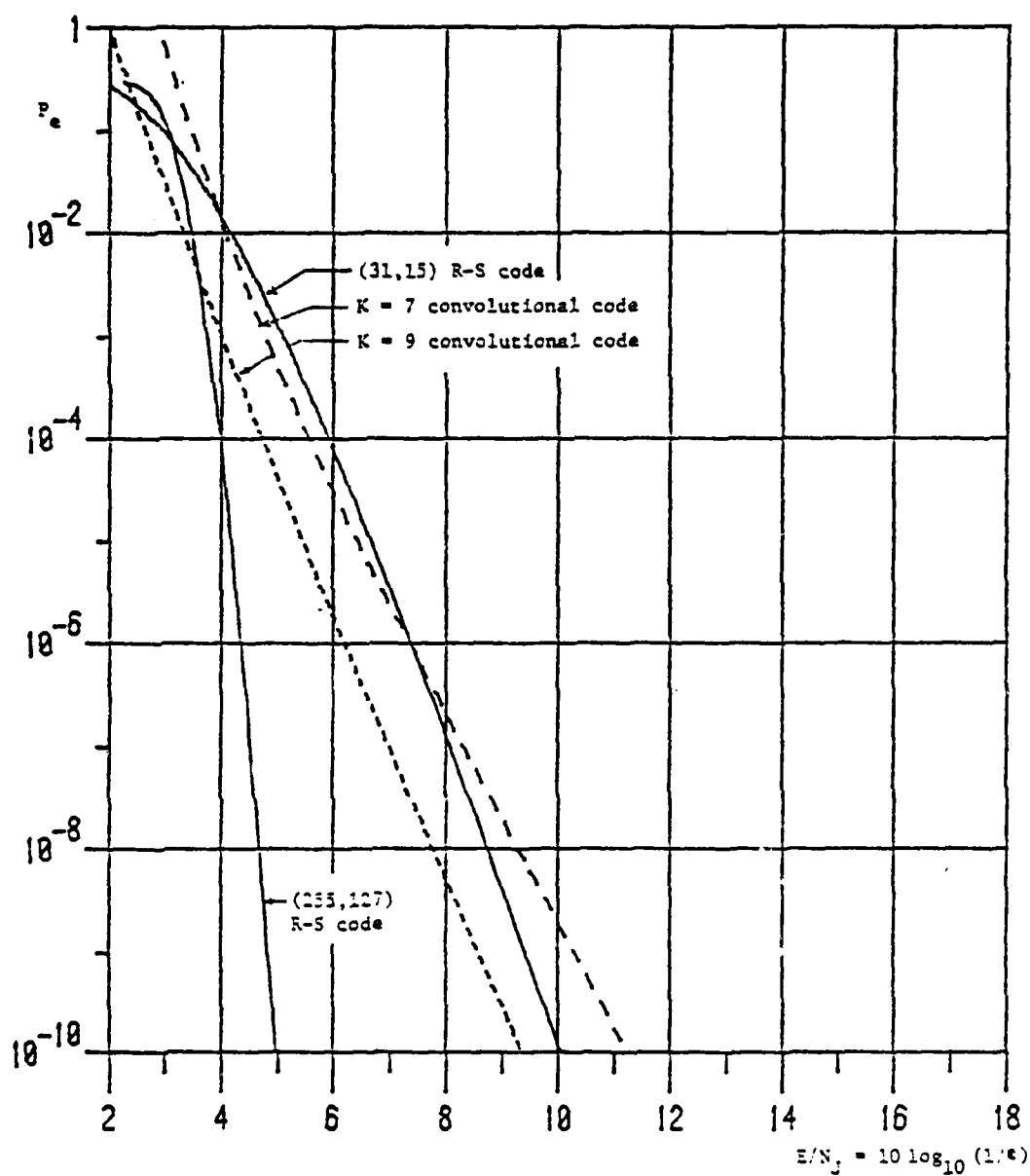


Figure 2.3. Error probability of Reed-Solomon codes (solid lines) and convolutional codes (dashed lines) on the interference channel of example 1a (side information available).

symbols are erased the error probability is $\frac{1}{2}$. In Figure 2.3 we plot the bit error probability given in (2.39) for two convolutional codes of rate $\frac{1}{2}$. These codes are the constraint length 7 ($v=6$) and constraint length 9 ($v=8$) codes as given in Table B-2 of [9].

Consider now the case of no side information available. For R-S code the probability of a received symbol being in error p_s is

$$p_s = \epsilon(1 - 2^{-m}) = \epsilon(2^m - 1)/2^m. \quad (2.41)$$

The error probability $P_{e,s}$ of a decoded symbol with bounded distance decoding is

$$P_{e,s} = \sum_{j = \frac{n-k}{2} + 1}^n \binom{n}{j} p_s^j (1 - p_s)^{n-j}. \quad (2.42)$$

If there are more than $(n-k)/2$ errors the bounded distance decoder detects with high probability that too many errors have occurred. In this case the decoder sets the decoded symbol equal to the received symbols. The decoded bit error probability $P_{e,b}$ is then given by

$$P_{e,b} = \frac{\frac{1}{2}}{1 - (\frac{1}{2})^m} P_{e,s} = \frac{2^{m-1}}{2^m - 1} P_{e,s}. \quad (2.43)$$

We have plotted in Figure 2.4 $P_{e,b}$ for the (31,15) and the (255,127) R-S codes vs $10 \log_{10}(1/\epsilon)$ on channel $\Delta(5)$ and $\Delta(8)$ respectively.

The performance of the convolutional codes with interleaving on channel $\Delta(m)$ is the same as the performance of a convolutional code on $\Delta(1)$, a BSC with crossover probability $\epsilon/2$. For this we use the bound in (2.39) with P_j given by

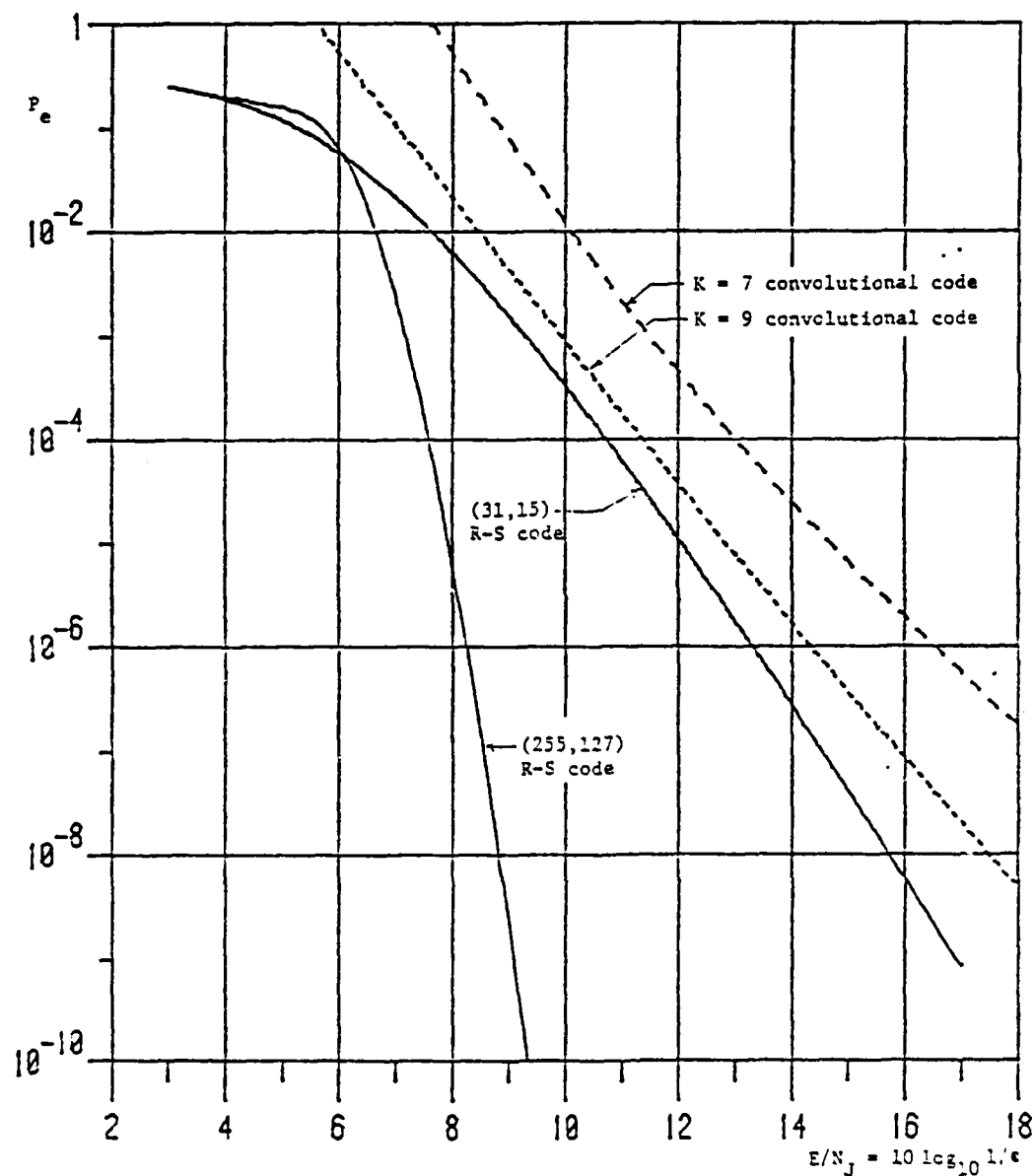


Figure 2.4. Error probability of Reed-Solomon codes (solid lines) and convolutional codes (dashed lines) on the interference channel of example 1a (side information not available).

$$P_j = \begin{cases} \sum_{i=(j+1)/2}^j \binom{j}{i} (\epsilon/2)^i (1 - \epsilon/2)^{j-i} & , \quad j \text{ odd} \\ \sum_{i=j/2}^{j-1} \binom{j-1}{i} (\epsilon/2)^i (1 - \epsilon/2)^{j-1-i} & , \quad j \text{ even} \end{cases} \quad (2.44)$$

This bound is plotted in Figure 2.4 versus $10 \log_{10}(1/\epsilon)$.

In comparing Figure 2.3 and Figure 2.4 we observe that the degradation for convolutional codes (used in conjunction with interleaving) between channels $\bar{\Delta}(m)$ and $\Delta(m)$ is much more than the degradation for R-S codes. Furthermore when side information is available the convolutional codes performance is comparable to the (31,15) R-S code. The (255,127) code is more complex and has better performance than the other codes. These results are not surprising since with side information available the channel capacity does not depend on the memory length so that interleaving should not cause a degradation in performance. However without side information available the capacity is an increasing function of the memory which implies that interleaving without side information should degrade the performance. The R-S codes which do not use interleaving perform better than the convolutional codes with interleaving when no side information is available as expected.

Other codes will be studied in the next two chapters.

CHAPTER 3

CODING FOR CHANNELS WITH PARTIAL-BAND

JAMMING AND COHERENT DEMODULATION

3.1 Introduction

In this chapter we consider a frequency-hopped spread-spectrum communication system subject to partial band-jamming. We consider both binary phase shift keying (BPSK) and M-ary orthogonal signaling forms of modulation. The modulated signal is frequency-hopped to produce the transmitted signal. The received signal is first frequency-dehopped and then coherently demodulated. The jammer adds noise to the signal over only a fraction of the frequency band the transmitter is using.

In Section 3.2 we describe the channel models we will use. In Section 3.3 we calculate the capacity of BPSK and M-ary orthogonal signaling in the presence of partial-band jamming. We consider channels with and without side information concerning the presence of the jammer and also channels with memory. In Section 3.4 we repeat these calculations for the cutoff rate. Finally in Section 3.5 we evaluate the performance of specific codes when side information is and is not available. This is then compared to the cutoff rate and the channel capacity.

3.2 Channel Models

In this section the channel models for frequency-hopped spread-spectrum communication using BPSK and M-ary orthogonal signals are given when there is partial-band jamming. As mentioned in Chapter 1 we treat the frequency hopper and dehopper as performing inverse operations on the modulated

signal. The output of the frequency dehopper consists of two additive terms. The first term corresponds to the received signal in the absence of noise, while the second term is due to the jamming noise and is nonzero only if there was jamming noise at the same frequency as the transmitted signal.

Consider frequency hopping with m symbols per hop. First we describe the channel for a particular hop for both BPSK and M-ary orthogonal signaling. For BPSK the channel input alphabet is $A = \{0,1\}$ while for M-ary orthogonal signaling $A = \{0,1,\dots,M-1\}$. Assume that the particular hop begins at time $t = 0$ and is of duration mT where T is the duration of a single symbol. Denote by X_j , $0 \leq j < m$, the random variable which takes values in A . When the input X_j , $0 \leq j < m$, takes the value $i \in A$, the data modulated signal $\hat{s}_i(t - jT)$ is the input to the frequency hopper during $jT \leq t \leq (j+1)T$. The signal $\hat{s}_i(t)$ is given by

$$\hat{s}_i(t) = \sqrt{2P} p_T(t) \sin(\omega_c t + (-1)^i \pi/2) \quad (3.1)$$

for BPSK while for M-ary orthogonal signaling $\{\hat{s}_i(t)\}_i \in A$ is any orthogonal signal set with each signal having power P , duration T and center frequency ω_c (see for example [20], Sec. 5-3). In (3.1) $p_T(t) = 1$ for $0 \leq t < T$ and $p_T(t) = 0$ otherwise, P is the signal power and ω_c is the center frequency of the modulated signal. The frequency hopper changes the frequency of the modulated signal in different hops to one of q frequencies according to a specified hopping pattern to produce the transmitted signal $s_i(t-jT)$ during the interval $jT \leq t < (j+1)T$, $0 \leq j < m$. For BPSK

$$s_i(t) = \sqrt{2P} p_T(t) \sin(\omega_c t + (-1)^i \pi/2) \quad (3.2)$$

and ω_l , $1 \leq l \leq q$ is one of the q possible frequencies of the hopping pattern. For M-ary orthogonal signaling $\{s_i(t)\}_{i \in A}$ is the same orthogonal signal set with center frequency ω_l instead of ω_c .

The jamming $j(t)$ consists of a sum of bandpass Gaussian processes:

$$j(t) = \sum_{i=1}^q j_i(t) \quad (3.3)$$

where the process $\{j_i(t); 0 \leq t < \infty\}$ is a bandpass Gaussian process with center frequency ω_i , $1 \leq i \leq q$, the q distinct frequencies of the hopping pattern. Let $S(\omega)$ be a low pass spectral density, i.e. $S(\omega) = 0$ for $|\omega| > \omega_L$ for some ω_L . We make the simplifying assumption that if $j_i(t)$ has nonzero power then $S(\omega - \omega_i)$, is the shape of its spectral density. Each process which has nonzero power has identical statistics and thus the power in each process is the same. In Appendix B we show that if the receiver has side information concerning which frequencies are jammed and at what power levels then in fact the worst case jamming strategy is for the jammer to place equal amounts of power in a fraction of the possible transmitted frequencies bands and no power in the remaining fraction.

When $s_i(t - jT)$ is transmitted, $0 \leq j < m$, the received signal $r(t)$ consists of the sum of the transmitted signal and the jamming signal:

$$r(t) = s_i(t - jT) + j(t), \quad jT \leq t \leq (j+1)T \quad (3.4)$$

(Here we assume, without loss of generality that all time delays are zero.)

The signal $\hat{r}(t)$ at the output of the frequency dehopper is then given by

$$\hat{r}(t) = \hat{s}_i(t - jT) + \hat{j}_l(t) \quad jT \leq t \leq (j+1)T \quad (3.5)$$

where $\hat{s}_i(t - jT)$ is the modulated signal and $\hat{j}_\ell(t)$ is the bandpass process with spectral density $S(\omega - \omega_\ell)$ obtained from $j(t)$ when $j(t)$ is frequency translated by $\omega_\ell - \omega_L$ and then filtered by an ideal bandpass filter with center frequency ω_c and bandwidth $2\omega_L$. Here ω_L is chosen so that $\hat{s}_i(t)$ is essentially unaltered when passed through an ideal lowpass filter with cutoff frequency ω_L . With probability p , $j_\ell(t)$ has nonzero power. A detailed model for the frequency hopper and dehopper is given in [13].

The models for the jamming signal and transmitted signal have several implicit assumptions that should be clarified. First, it is assumed that the jamming signal is a stationary random process. Second, it is assumed that the transmitter does not know which frequencies are being jammed with nonzero power. If the transmitter knows which frequencies are being jammed, the transmitter could put more power in those frequencies jammed and less in the frequencies unjammed. However, if the jammer knows the transmitter is putting more power in a particular set of frequencies, the jammer might wish to change the frequencies being jammed periodically in which case the transmitter might not be able to determine which frequencies are jammed at a particular time. Assuming that $j(t)$ is a stationary random process and that the transmitter does not know the frequencies being jammed is equivalent to allowing the jammer to change the frequencies being jammed often enough so that the transmitter cannot determine the jammed frequencies. A further assumption made is that during each hop either all the symbols are jammed with equal power or there is no jamming signal (with nonzero power) for all m symbols. This is perhaps the most restrictive assumption. If, however, the jamming signal changes much more slowly than the hopping rate then this is a reasonable assumption.

The demodulator has as input $\hat{r}(t)$ given in (3.5). For BPSK the demodulator computes the correlation Y between $r(t)$ and $s_1(t)$

$$Y_j = \gamma \int_{jT}^{(j+1)T} \hat{r}(t) \cos \omega_c t dt, \quad 0 \leq j < m, \quad (3.6)$$

where γ is a normalization constant to be defined later. For M-ary orthogonal signaling the demodulator computes

$$Y_{i,j} = \gamma \int_{jT}^{(j+1)T} \hat{r}(t) \hat{s}_i(t - jT) dt \quad 0 \leq j < m, \quad i \in A. \quad (3.7)$$

Thus for BPSK the channel is described by the input X_j and Y_j , $0 \leq j < m$.

For M-ary orthogonal signaling the channel is described by X_j and

$Y_{i,j}$, $i \in A$, $0 \leq j < m$. Since we assume that the jammer's signal is stationary and that the transmitter does not know which frequencies are being jammed the channel is memoryless from hop to hop so that the channel is completely described above.

To compute the distribution of the demodulator output we introduce a random variable Z which is nonzero if the jamming signal at the output of the frequency dehopper has nonzero power and is zero otherwise. Let $P\{Z = \sqrt{1/\rho}\} = \rho$ and $P\{Z = 0\} = 1 - \rho$. Then we can describe the signal $\hat{r}(t)$ at the output of the frequency dehopper by

$$\hat{r}(t) = \hat{s}_1(t - jT) + Z \cdot \hat{j}(t) \quad (3.8)$$

where $\hat{j}(t)$ is a bandpass Gaussian process with spectral density $S(\omega - \omega_c)$.

We now assume that $S(\omega - \omega_c)$ is flat in the interval $[\omega_c - \omega_L, \omega_c + \omega_L]$ with two sided density $\frac{1}{2} N_j$

For BPSK Y_j in (3.6) with $\gamma = (4/N_J T)^{\frac{1}{2}}$ is a random variable given by

$$Y_j = \sqrt{\frac{2E}{N_J}} (-1)^i + Z \cdot \eta \quad (3.9)$$

where $E = PT$ is the energy per symbol and η is a zero mean Gaussian random variable independent of Z with variance 1. Thus $Z\eta$ also has mean square 1. The density of Y_j given $X_j = i$ and $Z = \sqrt{1/\rho}$ (jammer on) is given by

$$p(y_i | X = i, Z = \sqrt{1/\rho}) = (2\pi)^{-\frac{1}{2}} \cdot \exp\left\{-\frac{1}{2}\left(y_i - \alpha \sqrt{\frac{2E_0}{N_J}}\right)^2\right\} \quad (3.10)$$

with $\alpha = (-1)^i$. When $Z = 0$ (jammer off) we have

$$P\{Y_j = \sqrt{2E/N_J} (-1)^i | X_j = i, Z = 0\} = 1 \quad (3.11)$$

Note that if $Y_j \neq \sqrt{2E/N_J} (-1)^i$ then with probability 1 the jammer was on ($Z = \sqrt{1/\rho}$). Using this test the receiver can tell whether or not the jammer was on during a particular hop. In this case we say the receiver has side information available. However, the receiver may just decide $X_j = 1$ if $Y_j < 0$ and $X_j = 0$ otherwise. In this case we say the receiver makes hard decisions and disregards the side information. Alternatively the receiver may make hard decisions and retain the side information.

For M-ary orthogonal signaling $Y_{i,j}$ in (3.7) with $\gamma = (2/N_J T)^{\frac{1}{2}}$ and $X_j = i$ is given by

$$Y_{k,j} = \sqrt{\frac{2E}{N_J}} \delta_{k,i} + Z \cdot \eta \quad k = 0, 1, \dots, M-1 \quad (3.12)$$

where E is the energy of each signal in the set, Z and η are the same as before and $\delta_{k,i} = 1$ if $i = k$ and $\delta_{k,i} = 0$ otherwise. The density of $Y_{k,j}$ given $X_j = i$ and $Z = \sqrt{1/\rho}$ is given by (3.10) with $\alpha = \delta_{k,i}$. If $Z=0$

$$P\{Y_{k,j} = \sqrt{\frac{2E}{N_J}} \delta_{k,i} | X_j = 1, Z = 0\} = 1 \quad (3.13)$$

Thus side information is available by checking if $Y_{k,j} = \sqrt{\frac{2E}{N_J}} \delta_{k,i}$ for some $i \in A$. Hard decisions correspond to deciding $X_j = 1$ if $Y_{1,j} > Y_{k,j}$ for all $k \neq 1$. We consider hard decisions both with and without side information available.

3.3 Channel Capacity

In this section we derive expressions for the capacity of the channels described in the previous section. The capacity is found from the game theoretic formulation of Chapter 2 with the jammer choosing the duty factor ρ . We compare this to the case of uniform jamming ($\rho = 1$). We conclude that provided codes with rate less than some critical rate are used uniform jamming is the worst case jamming strategy.

First consider BPSK and side information available to the receiver. There are two binary input channels involved here. When the jammer is on, the channel is just an additive Gaussian noise channel with signal energy-to-noise variance ratio $2E\rho/N_J$. The capacity $C(E\rho/N_J)$ of this component channel is achieved with a uniform distribution on A and is given by ([6] [27, Problem 4.14])

$$C(x) = \{x^2 - \int_{-\infty}^{\infty} g(t) \ln \cosh(x^2 + tx) dt\} / \ln 2 \quad (3.14)$$

where $g(t)$ is the density of a zero-mean, unit variance Gaussian random variable given by

$$g(t) = (2\pi)^{-1/2} e^{-1/2 t^2} \quad (3.15)$$

When the jammer is off the component channel is a binary noiseless channel with capacity 1 achieved by a uniform distribution on A. Thus both component channels have the same input distribution achieving the component capacity. In this case from (2.18) the capacity of the composite channel is independent of the memory length m of the channel. Thus the capacity $\bar{C}(E/N_J)$ for BPSK with worst case partial-band jamming is given by

$$\bar{C}(E/N_J) = \min_{0 \leq \rho \leq 1} \{ \rho C(E\rho/N_J) + (1-\rho) \} \quad (3.16)$$

The minimum in (3.16) can be found numerically or by setting the first derivative equal to zero:

$$\frac{\partial}{\partial \rho} \{ \rho C(E\rho/N_J) + (1-\rho) \} = 0$$

or

$$C(E\rho/N_J) + E\rho/N_J C'(E\rho/N_J) = 1 \quad (3.17)$$

where $C'(x) = \partial C(x)/\partial x$. From (3.17) we can determine the dependence of the worst case $\rho = \rho^*$ on the signal-to-noise ratio E/N_J as

$$\rho^* = \begin{cases} 1 & E/N_J < \alpha \\ \frac{\alpha}{E/N_J} & E/N_J \geq \alpha \end{cases} \quad (3.18)$$

where α is the solution of

$$C(\alpha) + \alpha C'(\alpha) = 1 \quad (3.19)$$

Using (3.18) in (3.16) we obtain

$$\bar{C}(E/N_J) = \begin{cases} C(E/N_J) & E/N_J < \alpha \\ 1 - \frac{\alpha - \alpha C(\alpha)}{E/N_J} & E/N_J \geq \alpha \end{cases} \quad (3.20)$$

Solving (3.19) we find that $\alpha = 1.649$ and $C(\alpha) = 0.655$. If we now have a different type of receiver capacity $\hat{C}(\beta)$ in the presence of additive Gaussian noise with signal-to-noise ratio β then with partial-band jamming (3.16)-(3.20) are valid with C replaced by $\hat{C}$. For BPSK with hard decision receiver and additive Gaussian noise the error probability is given by $Q(\sqrt{2E/N_J})$ where $Q(x) = \int_x^\infty g(t)dt$. The capacity is then given by [27]

$$C_2(\beta) = 1 - H_2(Q(\sqrt{2\beta})) \quad (3.21)$$

where $\beta = E/N_J$. Using (3.21) in (3.19) and solving for α we find $\alpha_2 = 2.156$ and $C_2(\alpha_2) = 0.630$. Thus for BPSK with hard decisions and side information the capacity $\bar{C}_2(E/N_J)$ is given by

$$\bar{C}_2(E/N_J) = \begin{cases} C_2(E/N_J) & E/N_J < \alpha_2 \\ 1 - \frac{\alpha_2 - \alpha_2 C_2(\alpha_2)}{E/N_J} & E/N_J \geq \alpha_2 \end{cases} \quad (3.22)$$

Now consider the case of no side information available and hard decisions. Since side information is no longer available the capacity is no longer independent of the memory. However this channel fits exactly the channel model in the example of Section 2.5 with $\epsilon = \rho$ and $f(\rho) = Q(\sqrt{2E\rho/N_J})$ so that the capacity is given by (2.35) and (2.36). The minimization in

(2.34) must in general be done numerically. However for the case of no memory ($m = 1$) the channel becomes a BSC with crossover probability $\bar{p}$ given by the average of the crossover probabilities of the two component channels:

$$\bar{p} = \rho \cdot Q(\sqrt{2E\rho/N_J}) + (1 - \rho) \cdot 0 = \rho Q(\sqrt{2E\rho/N_J}) \quad (3.23)$$

so that the capacity is the minimum of $1 - H_2(\bar{p})$ over $\rho \in [0, 1]$. Since $1 - H_2(x)$ is decreasing function of x we can equivalently maximize $\bar{p}$ over ρ

$$\max_{0 \leq \rho \leq 1} \bar{p} = \begin{cases} Q(\sqrt{2E\rho/N_J}) & E/N_J < \alpha_3 \\ \frac{\beta_3}{E/N_J} & E/N_J \geq \alpha_3 \end{cases} \quad (3.24)$$

in which case

$$C(E/N_J) = \min_{0 \leq \rho \leq 1} 1 - H_2(\bar{p}) = \begin{cases} 1 - H_2(Q(\sqrt{2E/N_J})) & E/N_J < \alpha_3 \\ 1 - H_2\left(\frac{\beta_3}{E/N_J}\right) & E/N_J \geq \alpha_3 \end{cases} \quad (3.25)$$

where $\alpha_3 = 0.709$, $\beta_3 = 0.08285$, and $C(\alpha_3) = 0.480$.

For M-ary orthogonal signaling we consider only the case of hard decisions. The probability $P_{e,s}$ of an error ($Y_{k,j} > Y_{i,j}$ for some $k \neq i$ when $X_j = i$) for uniform jamming can be calculated to be [1]

$$P_{e,s}(E/N_J) = (M-1) \int_{-\infty}^{\infty} \tilde{q}(t - \sqrt{2E/N_J}) \tilde{q}^{M-2}(t) g(t) dt \quad (3.26)$$

where $g(t)$ is given in (3.15) and $\tilde{q}(x) = 1 - Q(x)$. For the case of side information available and partial-band jamming the capacity can be calculated using (3.16)-(3.20) with $C(\alpha)$ replaced by $\hat{C}_M(P_{e,s}(\alpha))$ where

$$\hat{C}_M(P) = \frac{1}{\log_2 M} \{ \log_2 M + (1-P) \log_2 (1-P) + P \log_2 (P/(M-1)) \} . \quad (3.27)$$

The capacity (in M-ary units) is then given by

$$\bar{C}_M(E/N_J) = \begin{cases} \hat{C}_M(P_s(E/N_J)) & E/N_J < \gamma_M \\ 1 - \frac{\gamma_M - \gamma_M \hat{C}_M(P_s(\gamma_M))}{E/N_J} & E/N_J \geq \gamma_M \end{cases} \quad (3.28)$$

When side information is not available the capacity depends on the memory length. For $m = 1$ the channel is a memoryless M-ary symmetric channel (MSC) with symbol error probability given by the average error probabilities of the two component channels. As before the capacity is a decreasing function of the symbol error probability so that maximizing symbol error probability is equivalent to minimizing capacity. The maximum of the average error probability $\bar{P}_{e,s}(E/N_J)$ is given by

$$\begin{aligned} \bar{P}_s(E/N_J) &= \max_{0 \leq \rho \leq 1} \{ \rho P_s(E\rho/N_J) \} \\ &= \begin{cases} P_s(E/N_J) & E/N_J < \lambda_M \\ \frac{\lambda_M P_s(\lambda_M)}{E/N_J} & E/N_J \geq \lambda_M \end{cases} . \end{aligned} \quad (3.29)$$

The capacity $C_M(E/N_J)$ is found by using (3.27) with $P = \bar{P}_s(E/N_J)$ given in (3.29). Thus

$$C_M(E/N_J) = \begin{cases} \hat{C}_M(P_s(E/N_J)) & E/N_J < \lambda_M \\ \hat{C}_M\left(\frac{\lambda_M P_s(\lambda_M)}{E/N_J}\right) & E/N_J \geq \lambda_M \end{cases} \quad (3.30)$$

The values of γ_M , $\bar{C}_M(\gamma_M)$, λ_M and $P_s(\lambda_M)$ are given in Table 3.1 for $M = 2^k$, $k = 1, 2, \dots, 8$.

Table 3.1. Values of constants used to determine capacities for M-ary orthogonal signaling.

M	γ_M	$\bar{C}_M(\gamma_M)$	λ_M	$P_s(\lambda_M)$	$C_M(\lambda_M)$
2	2.156	0.630	1.418	0.117	0.480
4	2.402	0.596	1.701	0.211	0.461
8	2.681	0.563	2.012	0.287	0.443
16	2.987	0.532	2.345	0.350	0.424
32	3.315	0.504	2.699	0.402	0.407
64	3.664	0.478	3.069	0.446	0.390
128	4.030	0.454	3.455	0.484	0.374
256	4.410	0.432	3.853	0.516	0.359

To interpret these results concerning the channel capacity we consider Theorem 2 of Chapter 2 which says that there exists codes with rate $r < C$, such that reliable communication (error probability less than λ) is possible. In all cases considered here the capacity is a function of E/N_J the symbol

signal-to-noise ratio (SNR). If we use codes of rate r then the bit signal-to-noise ratio E_b/N_J is given by

$$E_b/N_J = (E/N_J) \cdot (1/r \log_2 M)$$

where $M = 2$ for BPSK. Thus for reliable communication we must have

$$r < C(E_b/N_J \cdot r \log_2 M)$$

or

$$E_b/N_J > C^{-1}(r)/r \log_2 M \quad (3.31)$$

where $C^{-1}(r)$ is the inverse function of the capacity. The performance of a particular modulation-demodulation scheme can be measured by the right hand side (RHS) of (3.31) and determines the bit signal-to-noise ratio needed for reliable communication.

For soft decision BPSK the capacity with side information is given by (3.20). In Figure 3.1 we plot RHS of (3.31) with C given in (3.20). This is compared to the bit SNR needed to achieve capacity for uniform jamming. Note that for small enough code rate ($r < 0.655$) uniform jamming is the optimal strategy for the jammer.

For hard decisions BPSK (binary output quantization) we have two cases to consider. With side information available, so that capacity is independent of memory length, the minimum E_b/N_J as a function of r is given in Figure 3.2. The rate below which uniform jamming is optimum is 0.630. When side information is available the capacity depends on the memory length. For $m = 1$ the capacity is given by (3.25) for $1 < m < \infty$ the

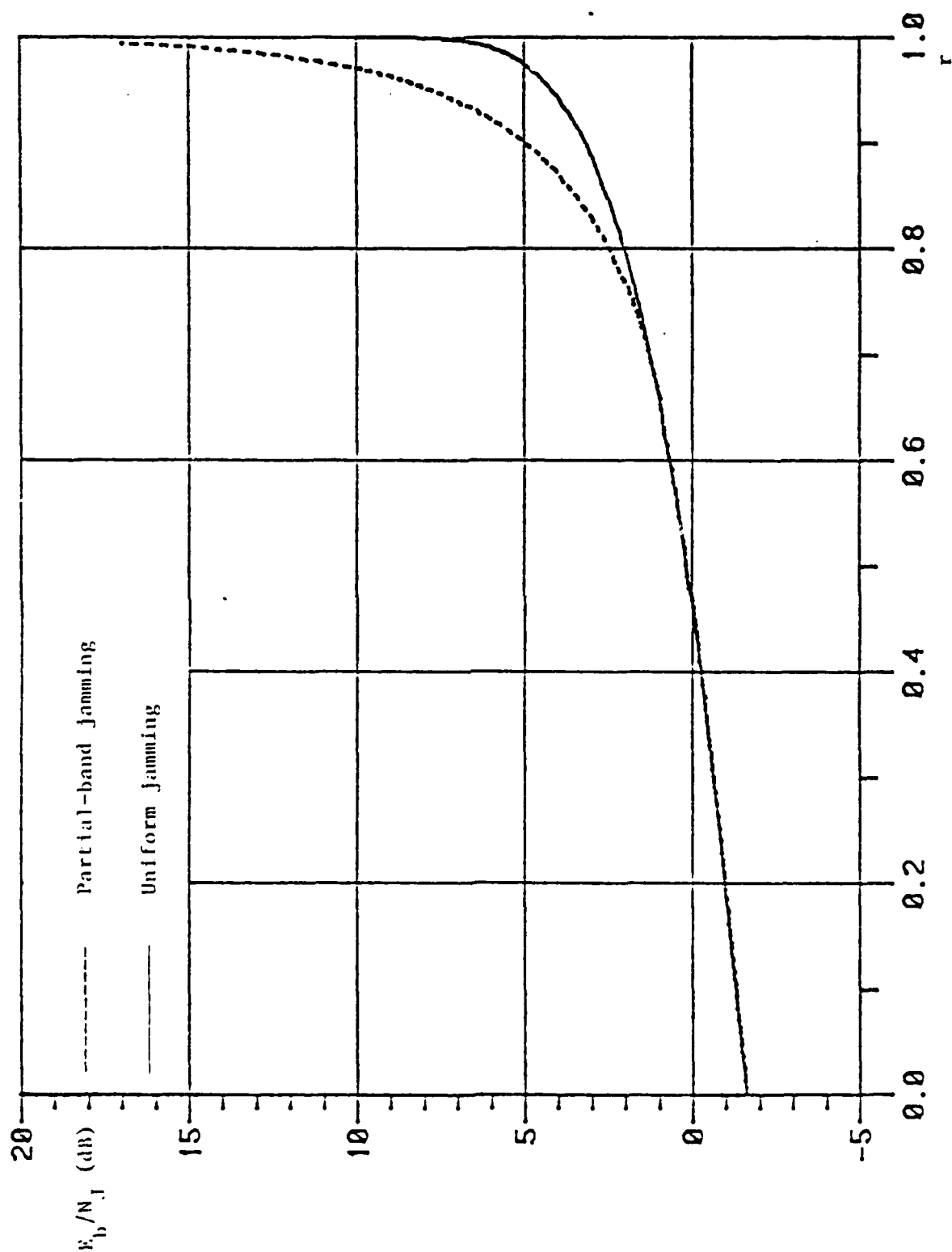


Figure 3.1. E_b/N_j needed to achieve capacity for BPSK with soft decisions and partial-band jamming (side information available).

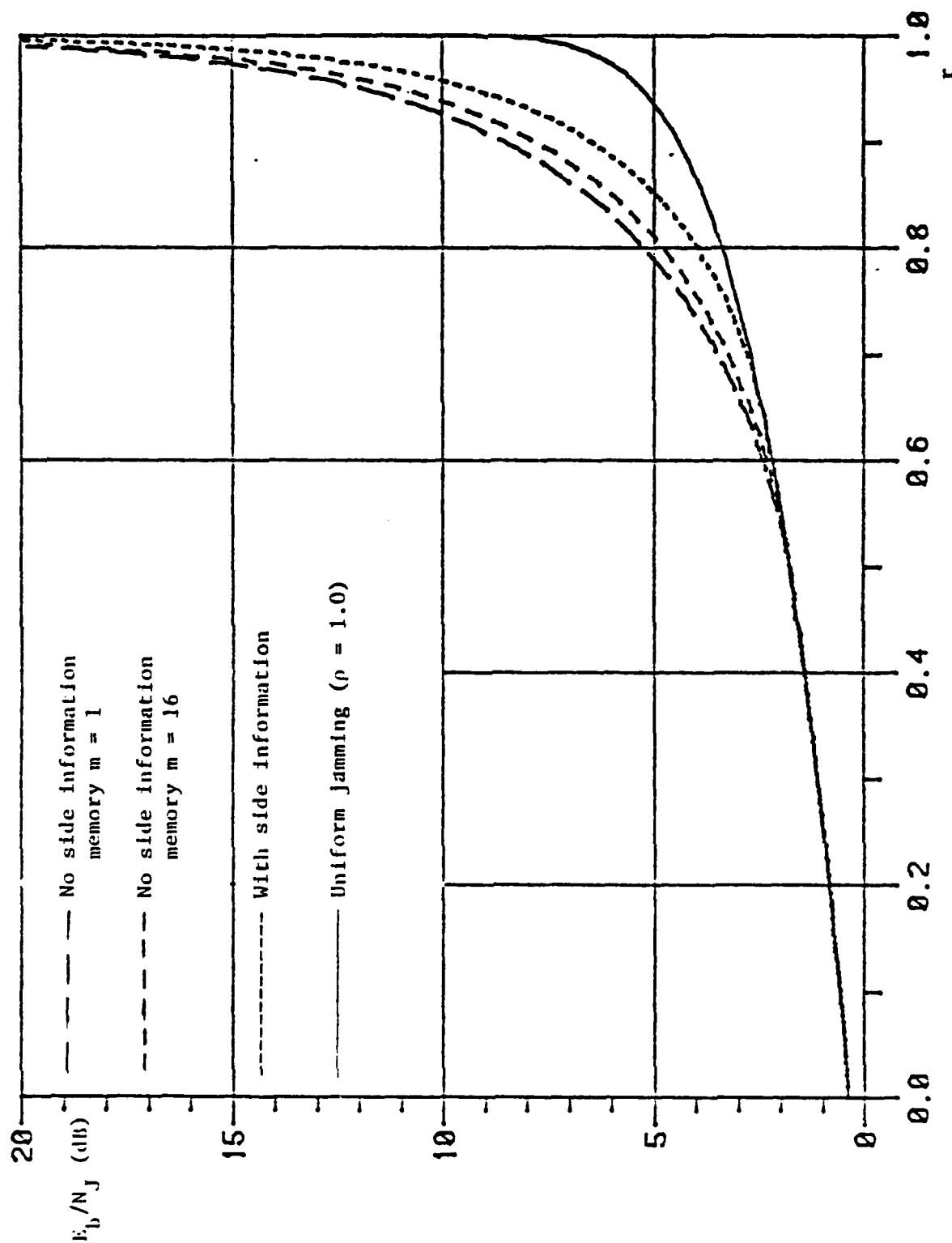


Figure 3.2. E_b/N_J needed to achieve capacity for BPSK with hard decisions and partial-band jamming.

capacity is given in (2.35) with $\epsilon = \rho$ and $\alpha_{m,k}$ given by

$$\alpha_{m,k} = \begin{cases} (1 - \rho) + \rho (1 - Q(\sqrt{2E_p/N_J}))^m & k = 0 \\ \rho Q(\sqrt{2E_p/N_J})^k (1 - Q(\sqrt{2E_p/N_J}))^{m-k} & k = 1, 2, \dots, m \end{cases} \quad (3.32)$$

The minimum in (2.35) no longer has the simple form of before. In Figure 3.2 we plot the E_b/N_J necessary for reliable communication for $m = 16$ without side information and E_b/N_J with side information.

For M-ary orthogonal signaling the corresponding curves for $m = 1$ (memoryless) and $M = 4, 8, 16, 32$ are shown in Figures 3.3-3.6. The rates below which uniform jamming is optimal are given in Table 3.1. The increase in E_b/N_J need to achieve capacity at low rates is due to the form of modulation employed. The increase for high rates is due to the decrease in the codes redundancy at these rates. M-ary orthogonal signaling can also be viewed as a form of coding. It is an orthogonal code with rate $(\log_2 M)/M$. If an outer code with rate r is used on the code words of the M-ary orthogonal code then the overall code rate r' is $r' = r \log_2 M/M$. Figures 3.3-3.6 could be plotted versus the overall r' instead of r , however, the same effect for low and high code rates would still be present. We could also compare these curves to those for BPSK to determine the loss incurred by using an orthogonal code as an inner code in a concatenated coding approach. Even though M-ary orthogonal signaling (for finite M) is less efficient than BPSK, we shall see that it can be combined with Reed-Solomon codes to provide performance comparable to BPSK.

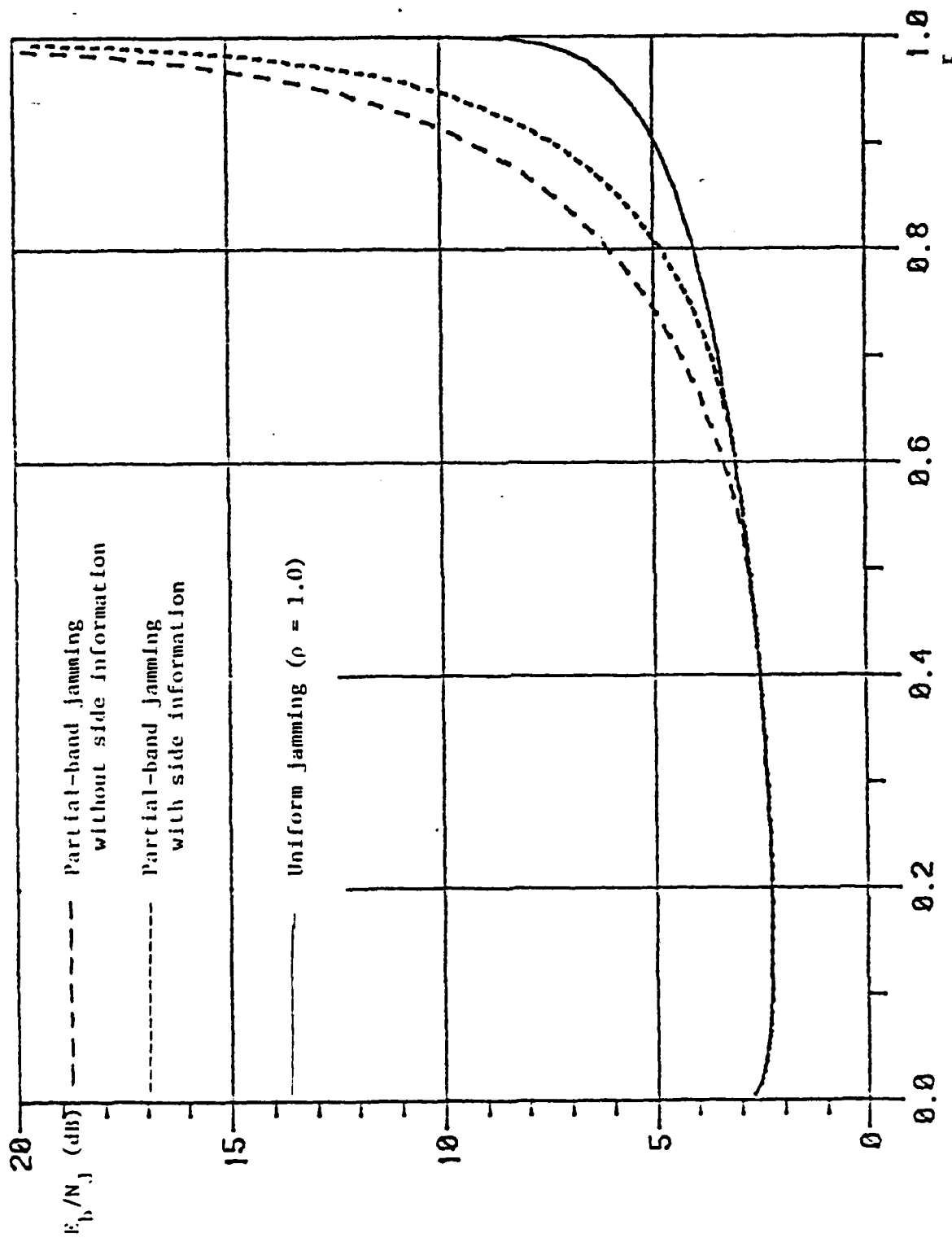


Figure 3.3. E_b/N_j needed to achieve capacity for 4-ary orthogonal signaling with partial-band jamming and hard decisions.

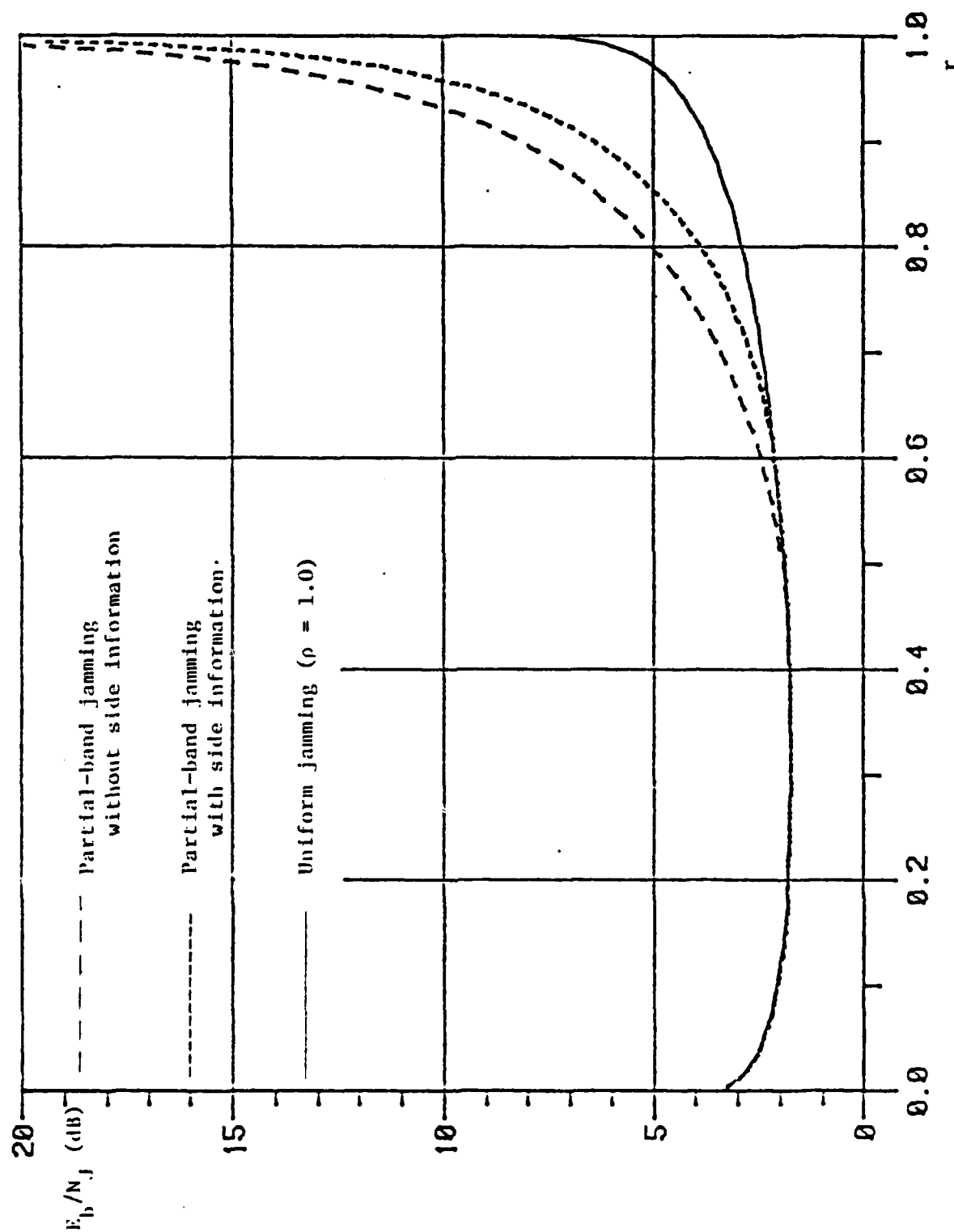


Figure 3.4. E_b/N_j needed to achieve capacity for 8-ary orthogonal signaling with partial-band jamming and hard decisions.

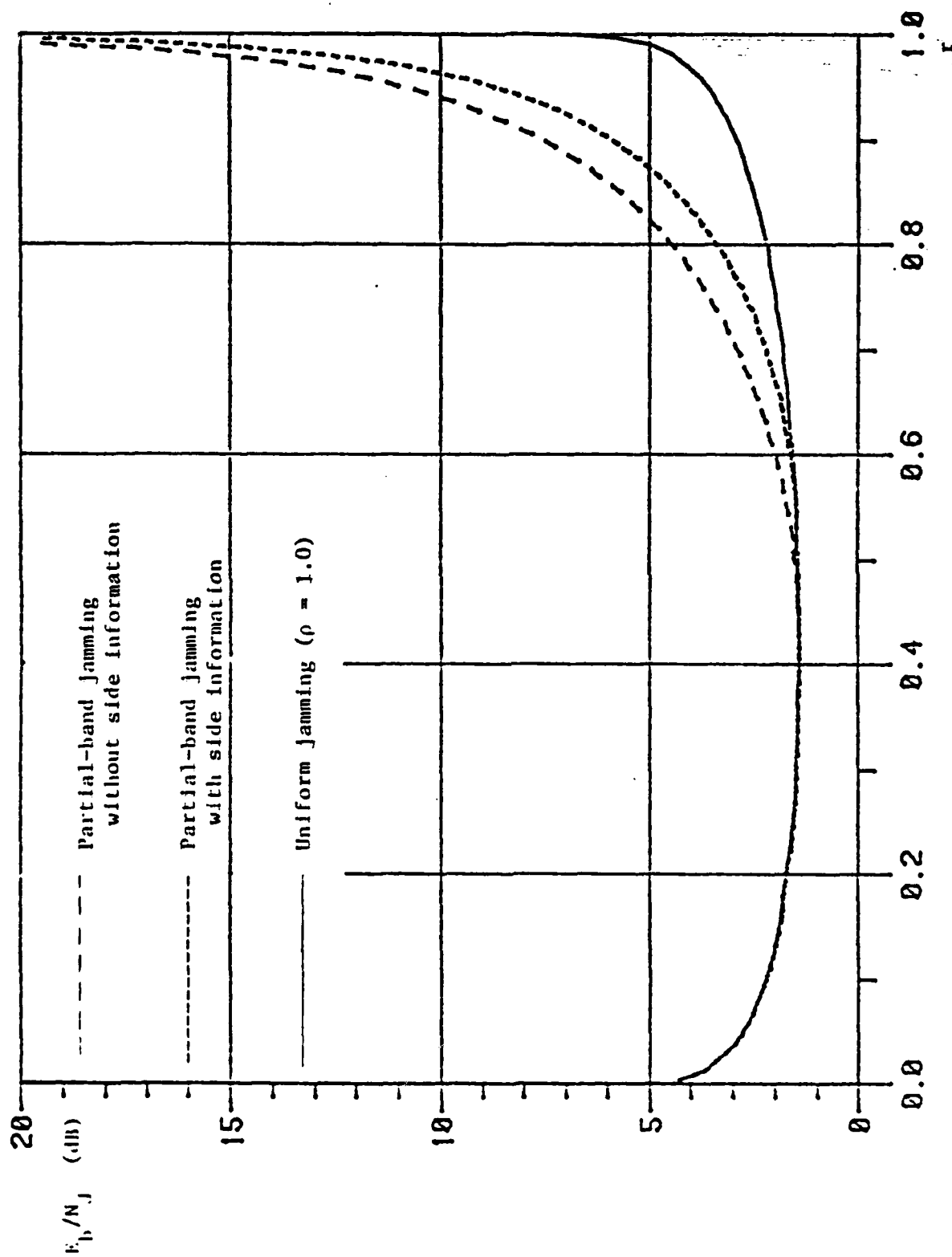


Figure 3.5. E_b/N_j needed to achieve capacity for 16-ary orthogonal signaling with partial-band jamming and hard decisions.

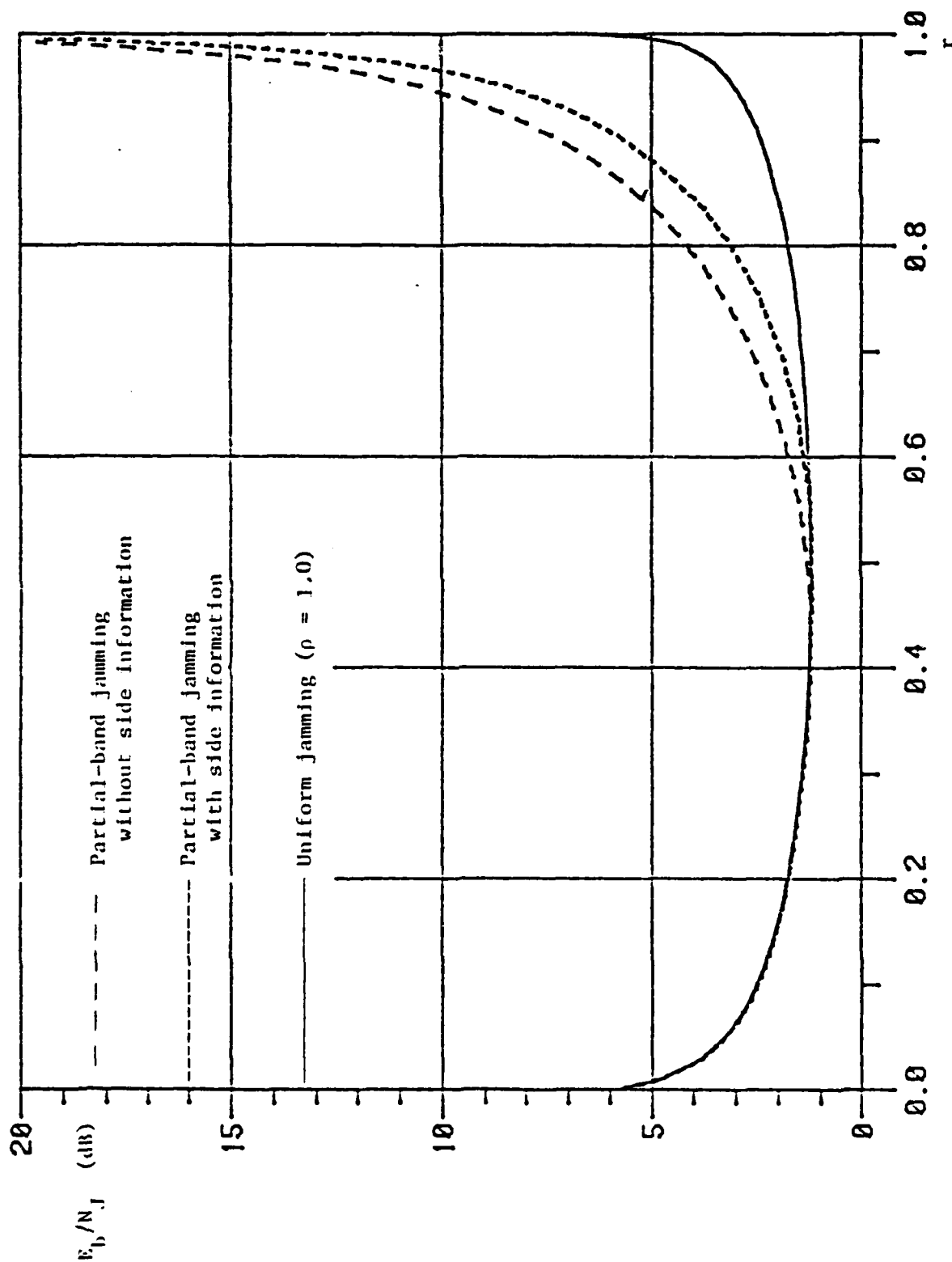


Figure 3.6. E_b/N_j needed to achieve capacity for 32-ary orthogonal signaling with partial-band jamming and hard decisions.

3.4 Channel Cutoff Rate

In this section we derive expressions for the computational cutoff rate for channels with partial-band jamming. The cutoff rate of BPSK with soft decisions, side information and memory has been calculated by Viterbi [43]. We extend these results to include BPSK with hard decisions with and without side information available. We also calculate the cutoff rate for M-ary orthogonal signaling with soft and hard decisions.

Consider first the case of side information available. From (2.28) the cutoff rate with side information and memory m is given by

$$\bar{R}_0(m) = -\frac{1}{m} \log_2 E\{J^m(s)\} \quad (3.33)$$

where

$$J(s) = 2^{-R_{0,s}} \quad (3.34)$$

and $R_{0,s}$ is the cutoff rate of the component channel Δ_s . However (3.33) and (3.34) are valid only when the distribution that achieves $R_{0,s}$ in (2.27) is the same for all component channels. This assumption will be true for all channels considered here. Viterbi [43] has computed the cutoff rate for the case of BPSK with soft decisions and partial band jamming as

$$\bar{R}_0(m) = \min_{0 \leq \rho \leq 1} \left\{ 1 - \frac{1}{m} \log_2 \left((1-\rho) + \rho \left[1 + e^{-\rho E/N_J} \right]^m \right) \right\} \quad (3.35)$$

$$= \begin{cases} 1 - \log_2 \left[1 + e^{-E/N_J} \right] & E/N_J < \nu_m \\ 1 - \frac{1}{m} \log_2 \left[1 + \frac{\mu_m}{E/N_J} \right] & E/N_J \geq \nu_m \end{cases} \quad (3.36)$$

The constants in (3.36) are given in Table 3.2.

Table 3.2. Constants for computing cutoff rate for BPSK with partial-band jamming.

m	μ_m	ν_m	γ_m	Γ_m
1	.368	1.000	0.6038	1.707
2	.882	0.850	1.439	1.443
3	1.646	0.759	2.670	1.187
4	2.854	0.579	4.603	0.963
5	4.856	0.475	7.796	0.784
6	8.287	0.395	13.258	0.646
7	14.303	0.335	22.819	0.544
8	25.018	0.288	39.829	0.467

For M-ary orthogonal signaling with uniform jamming, $m = 1$ and soft decisions the channel cutoff rate is given by [16]

$$R_0(M) = -\log_2 \left\{ \left[1 + (M-1)e^{-E/2N_J} \right] / M \right\} \quad (3.37)$$

where R_0 is measured in bits per transmission. For partial-band jamming with side information available, memory $m = 1$ and soft decisions the cutoff rate $\bar{R}_0(M)$ from (3.33) and (3.34) is given by

$$\bar{R}_0(M) = \min_{0 \leq \rho \leq 1} \left\{ \log_2 M - \log_2 \left[1 - \rho + \rho \left(1 + (M-1)e^{-E\rho/2N_J} \right) \right] \right\} \quad (3.38)$$

The minimization can be done easily to give the worst case $\rho = \rho^*$ for partial-band jamming as

$$\rho^* = \begin{cases} 1 & E/N_J < 2 \\ \frac{2}{E/N_J} & E/N_J \geq 2 \end{cases} \quad (3.39)$$

so that

$$\bar{R}_0(M) = \begin{cases} \log_2 M - \log \left[1 + (M-1)e^{-E/2N_J} \right] & , E/N_J < 2 \\ \log_2 M - \log \left[1 + 2(M-1)e^{-1/(E/N_J)} \right] & , E/N_J \geq 2 \end{cases} \quad (3.40)$$

It is interesting to compute the limit as $M \rightarrow \infty$ in (3.40).

$$\lim_{M \rightarrow \infty} \bar{R}_0(M) = \begin{cases} (E/2N_J) \log_2 e & , E/N_J \leq 2 \\ \log_2 (e E/2N_J) & , E/N_J \geq 2 \end{cases} \quad (3.41)$$

while for uniform jamming ($\rho = 1$) the limit as $M \rightarrow \infty$ of R_0 is just $(E/2N_J) \log_2 e$. Thus for uniform jamming R_0 is a linearly increasing function of E/N_J while for partial-band jamming R_0 is increasing logarithmically. Similar calculations can be done for the case of memory $m > 1$ and M-ary orthogonal signaling.

For BPSK and hard decisions the error probability with uniform jamming is given by

$$p = Q(\sqrt{2E/N_J}) \quad (3.42)$$

and the cutoff rate by

$$\begin{aligned} R_0 &= 1 - \log_2(1 + 2\sqrt{p(1-p)}) \\ &= -\log_2(1 + 2\sqrt{p(1-p)})/2 \end{aligned} \quad (3.43)$$

From (3.33) we can compute the cutoff rate $\bar{R}_0^{(2)}(m)$ for partial-band jamming with side information, hard decisions and memory m as

$$\bar{R}_0^{(2)}(m) = \min_{0 \leq \rho \leq 1} \left\{ 1 - \frac{1}{m} \log_2 [1 - \rho + \rho (1 + 2\sqrt{\hat{p}(1-\hat{p})})^m] \right\} \quad (3.44)$$

where $\hat{p} = Q(\sqrt{2E\rho/N_J})$. The minimization in (3.45) can be done to yield

$$\bar{R}_0^{(2)}(m) = \begin{cases} 1 - \log_2(1 + 2\sqrt{\hat{p}(1-\hat{p})}) & E/N_J < \Gamma_m \\ 1 - \frac{1}{m} \log_2 \left(1 + \frac{\gamma_m}{E/N_J} \right) & E/N_J \geq \Gamma_m \end{cases} \quad (3.45)$$

The constants γ_m and Γ_m are given in Table 3.2 for $1 \leq m \leq 8$.

When no side information is available the channel is simply a block m memoryless channel. The cutoff rate is given by (see (2.31))

$$R_0(m) = \min_{0 \leq \rho \leq 1} \left\{ 1 - \frac{2}{m} \log_2 \sum_{k=0}^m \binom{m}{k} \alpha_{m,k} \right\} \quad (3.46)$$

with $\alpha_{m,k}$ given in (3.32). For $m = 1$, however, the channel is simply a BSC with error probability $\rho Q(\sqrt{2E\rho/N_J})$ so that minimizing the cutoff rate is equivalent to maximizing the error probability. This maximum is given by

$$\bar{\rho} = \max_{0 \leq \rho \leq 1} \rho Q(\sqrt{2E\rho/N_J}) = \begin{cases} Q(\sqrt{2E/N_J}) & , \quad E/N_J > 0.709 \\ \frac{0.08285}{E/N_J} & , \quad E/N_J \leq 0.709 \end{cases} \quad (3.47)$$

and the cutoff rate by using (3.47) in (3.43).

For M-ary orthogonal modulation with memory $m = 1$ and hard decisions the cutoff rate R_0 with uniform jamming is given by (measured in M-ary units)

$$R_0 = -\log_M \left[\frac{1}{M} \left(\sqrt{1-P_s(E/N_J)} + \sqrt{(M-1)P_s(E/N_J)} \right)^2 \right] \quad (3.48)$$

so that the cutoff rate with partial-band jamming is given by

$$\begin{aligned} \bar{R}_0^{(2)}(M) &= \min_{0 \leq \rho \leq 1} \left\{ 1.0 - \log_M \left[(1-\rho) + \rho \left(\sqrt{1-P_s(E\rho/N_J)} + \sqrt{(M-1)P_s(E\rho/N_J)} \right)^2 \right] \right\} \quad (3.49) \\ &= \begin{cases} 1.0 - \log_M \left[\left(\sqrt{1-P_s(E/N_J)} + \sqrt{(M-1)P_s(E/N_J)} \right)^2 \right] & E/N_J < \alpha_M \\ 1.0 - \log_M \left[1 + \frac{\beta_M}{E/N_J} \right] & E/N_J \geq \alpha_M \end{cases} \quad (3.50) \end{aligned}$$

where α_M and β_M are given in Table 3.3. When no side information is available the cutoff rate is found by using (3.48) with P_s replaced by $\bar{P}_s$ given in (3.29).

Table 3.3. Constants used to determine $\bar{R}_0^{(2)}(M)$.

M	α_M	β_M
2	3.415	1.208
4	3.347	3.744
8	3.307	9.240
16	3.335	21.443
32	3.444	48.915
64	3.627	111.088

We interpret these results in the same way as we did for capacity. For all cases the cutoff rate $R_0(E/N_J)$ is a function of the symbol signal-to-noise ratio. If we use codes with rate $r < R_0(E/N_J)$ then we must have

$$E_b/N_J > R_0^{-1}(r)/r \cdot \log_2 M \quad (3.51)$$

for reliable communication (from cutoff rate considerations).

In Figure (3.7) we show the E_b/N_J needed to achieve R_0 for BPSK with soft decisions and side information available (memory 1). Both partial-band and uniform jamming cases are shown. For hard decisions with BPSK the three cases (i) partial-band jamming, no side information (ii) partial-band jamming with side information and (iii) uniform jamming are shown. In Figure 3.9 the case of hard decisions, side information and memory is considered for $m = 1, 2, 4, 8$. Notice that as m increases the necessary E_b/N_J also increases. For capacity we saw a decrease in E_b/N_J when memory was increased. For channels with memory capacity is a better measure of a channel reliability than the cutoff rate. In Figures 3.10 and 3.11 the E_b/N_J needed to achieve R_0 is shown for 16-ary and 32-ary orthogonal signaling with hard decisions.

3.5 Performance of Codes

In this section we compute the performance of specific codes on channels with partial-band jamming. We consider both BPSK and M-ary orthogonal signaling forms of modulation with coherent demodulation. Three different types of receivers are considered: (i) soft decisions, side information available, (ii) hard decisions, side information available, and (iii) hard decisions no side information available.

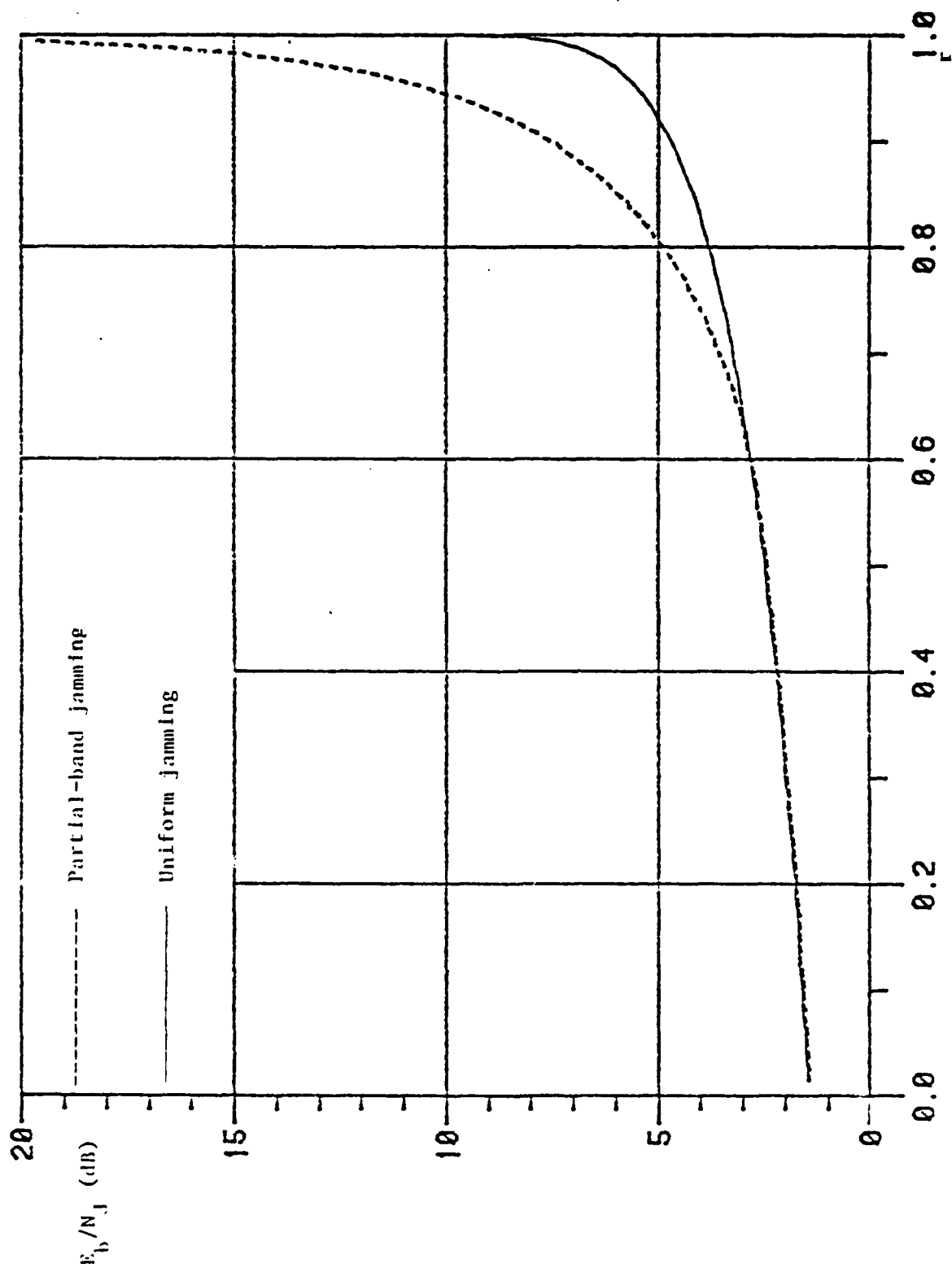


Figure 3.7. E_b/N_J needed to achieve cutoff rate for BPSK with soft decisions and partial-band jamming (side information available).

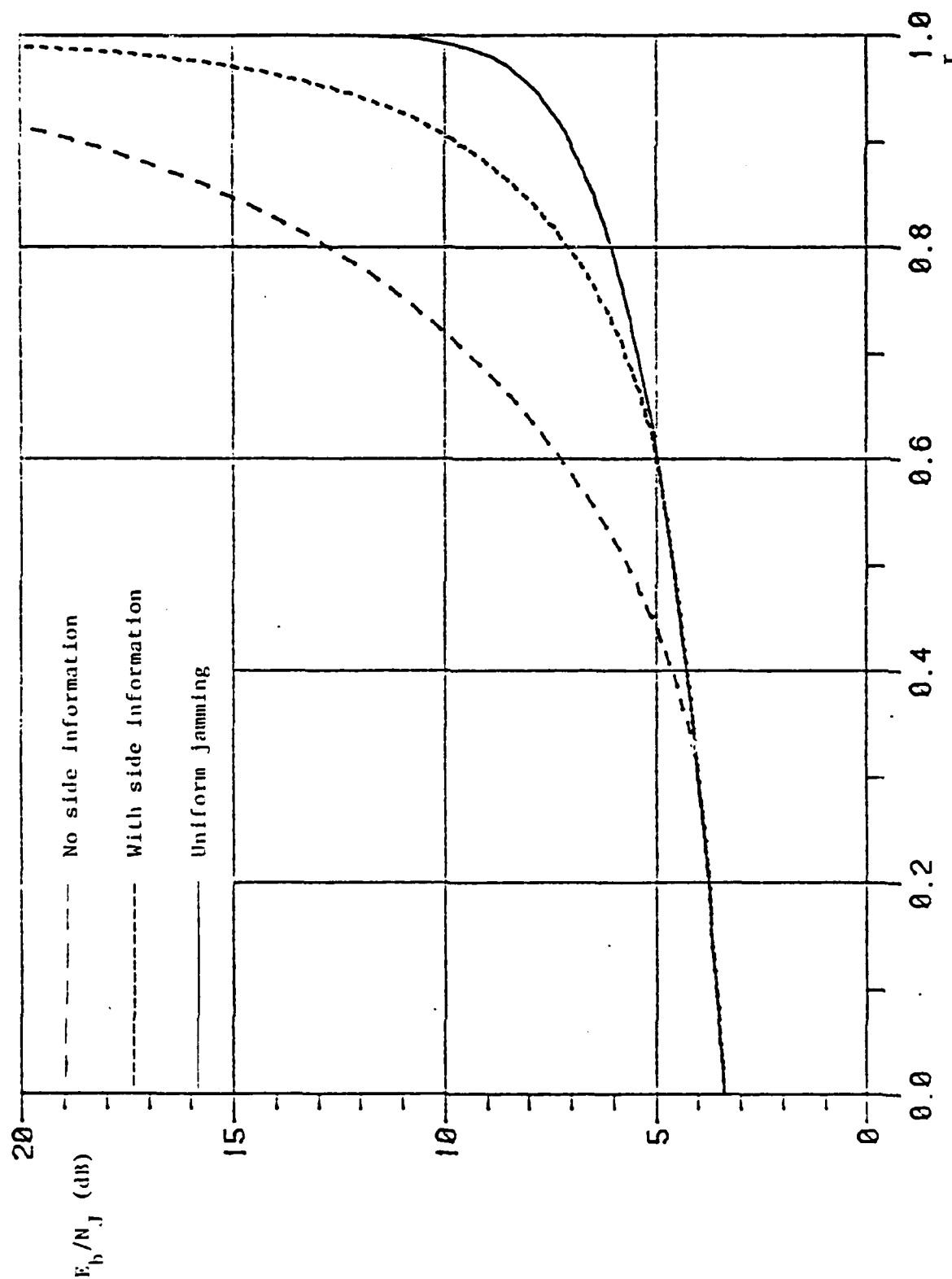


Figure 3.8. E_b/N_j needed to achieve error rates for BPSK with hard decisions and partial-band jamming.

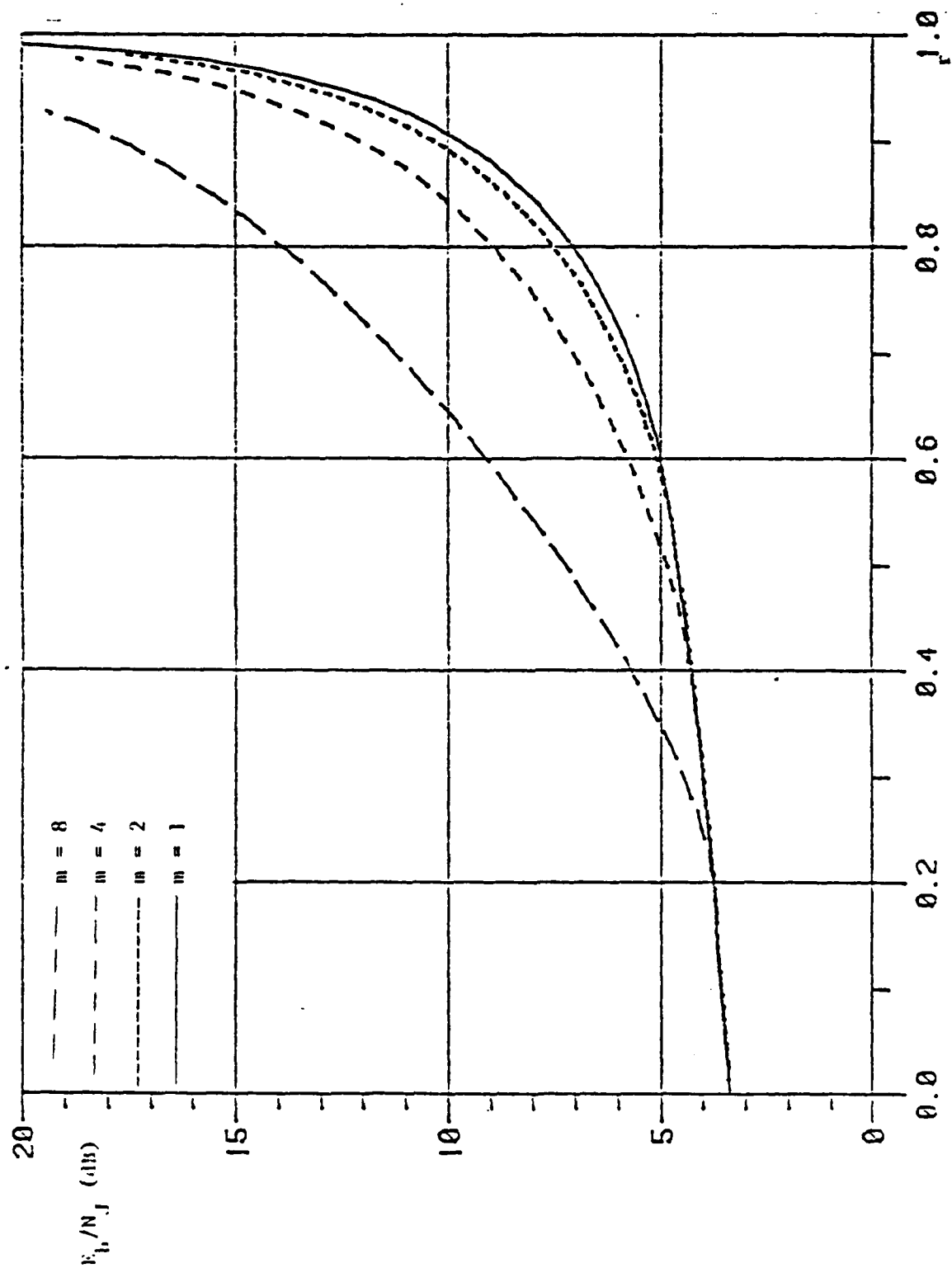


Figure 3.9. E_b/N_J needed to achieve cutoff rate for BPSK with hard decisions, side information available and memory m .

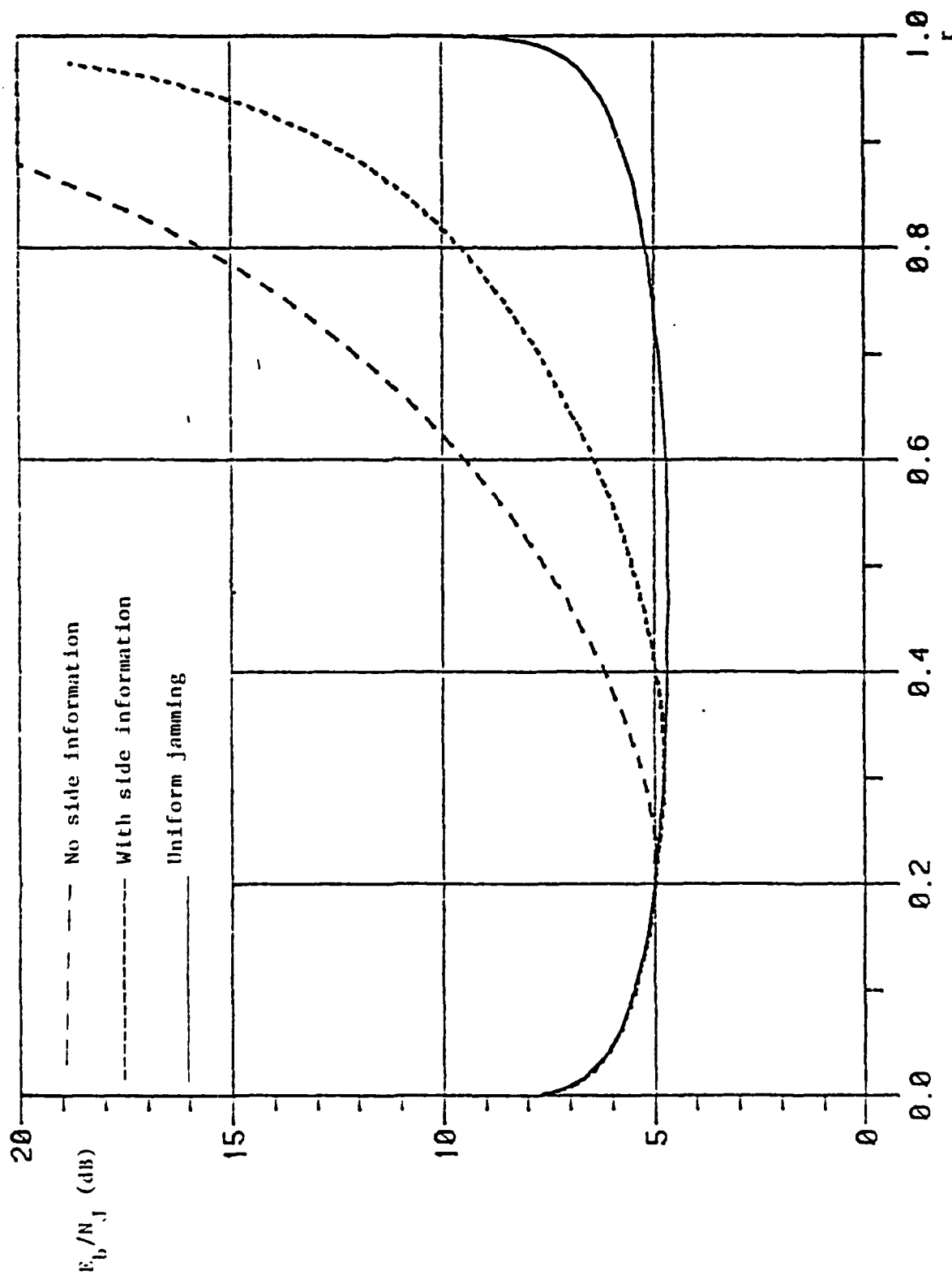


Figure 3.10. E_b/N_J needed to achieve cutoff rate for 16-ary orthogonal signaling with hard decisions and partial-band jamming.

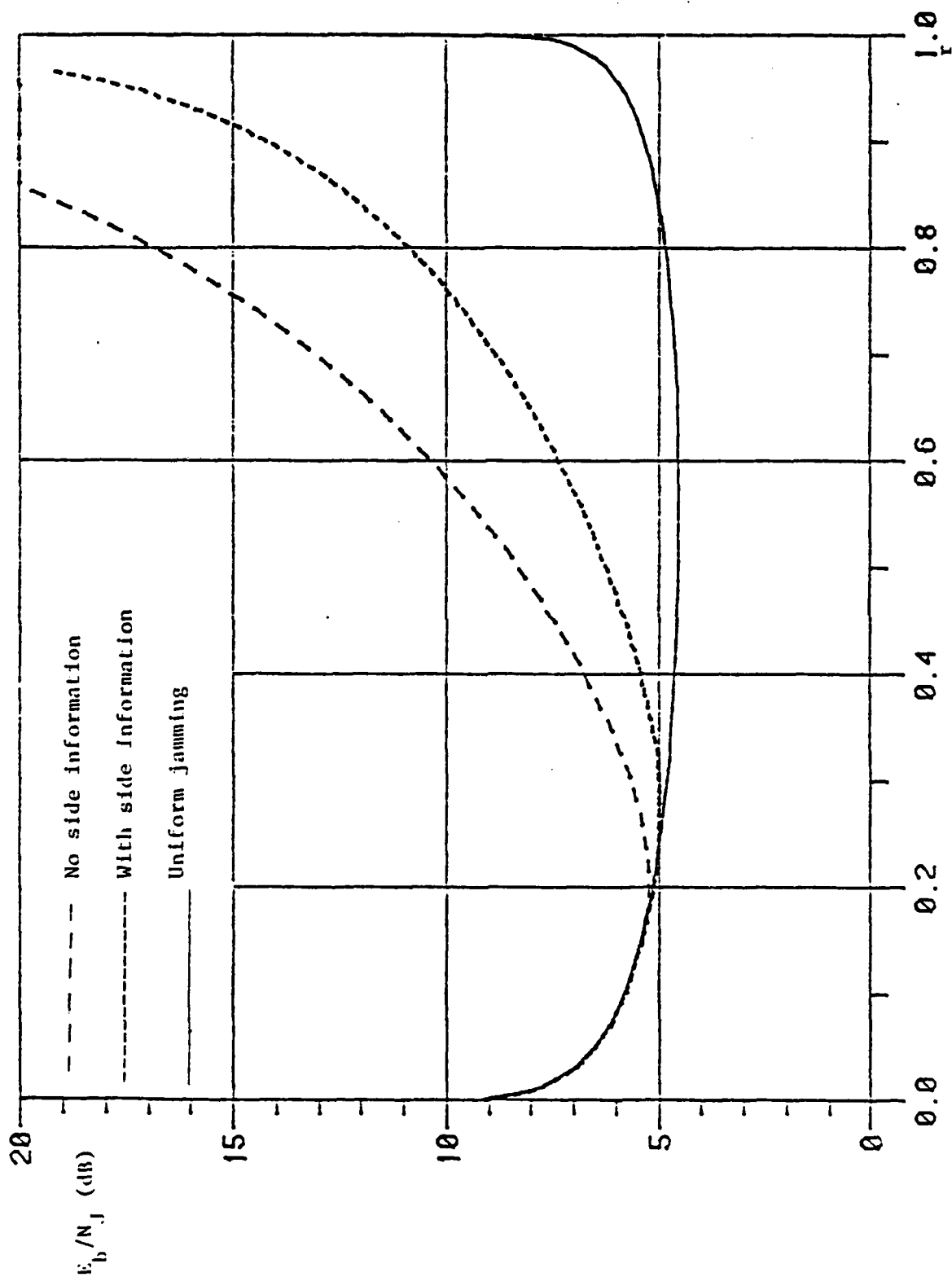


Figure 3.11. E_b/N_j needed to achieve cutoff rate for 32-ary orthogonal signaling with hard decisions and partial-band jamming.

There are several types of codes we consider in combination with the different types of modulation. We consider channels with memory ($m > 1$) and without memory ($m = 1$). One way of distinguishing codes is by the alphabet size of the code symbols. Codes which have symbols over alphabets larger than two are capable of treating symbols from an M-ary form of modulation as one symbol in the code. Binary codes can also be used with M-ary modulation by treating one symbol as $\log_2 M$ bits and encoding each bit separately. This is a form of interleaving and when used on channels without side information can degrade the channel reliability from capacity considerations. However the performance of specific codes must be evaluated since the overall performance depends also on the type of codes used on these channels.

Consider first M-ary orthogonal signaling with no memory ($m = 1$), no side information available and hard decisions. The symbol error probability for the worst-case partial-band jammer is given in (3.29). If we use R-S codes in conjunction with M-ary orthogonal modulation then the decoded symbol error probability $P_{e,s}$ can be found by using (3.29) in (2.42) with P_s in (2.42) replaced by $\bar{P}_s(E/N_J)$. The decoded bit error probability $P_{e,b}$ can then be computed as

$$P_{e,b} = \frac{1}{2} \frac{M}{M-1} P_{e,s} \quad (3.52)$$

Another type of code with alphabet size greater than 2 is the dual-k convolutional code [30], [44]. This code has alphabet size 2^k and can be used with M-ary modulation ($M = 2^k$). The performance of this code can be evaluated using (2.40). The summation in (2.40) can be approximated by the first several terms. The evaluation of (2.40) requires the calculation

of P_j , the error probability between two words differing in j symbols. This calculation for an M -ary symmetric channel is done in Appendix C.

A bound on (2.40) can be obtained by bounding P_j by D^j where for an M -ary symmetric channel with symbol error probability $\bar{P}_s$, D is given by [27, Prob. 7.10]

$$D = \left(\frac{M-2}{M-1}\right) \bar{P}_s + 2\sqrt{(1-\bar{P}_s)\bar{P}_s/(M-1)} \quad (3.53)$$

Using this bound on P_j the series in (2.40) can be summed for dual- k codes with rate $1/v$ to yield [30]

$$P_{e,s} < \frac{(2^k - 1)D^{2v}}{[1 - vD^{v-1} - (2^k - 1 - v)D^v]^2} \quad (3.54)$$

The bit error probability can be evaluated using (3.52). The w_j in (2.40) can be evaluated from (3.54) by expanding the denominator into a series in D . Doing this w_j is the coefficient of the term D^j .

Still another code which has code symbols of size greater than 2 is the length n repetition code. This simple code transmits each symbol n times in a row. The rate of this code is $1/n$. For a receiver with hard decisions the decoder counts the number of times the receiver decides each symbol was transmitted and then chooses the symbol that was decided upon the most. If there is a tie between 2 or more symbols the decoder chooses one randomly. The symbol error probability for these codes is derived in Appendix C for $1 \leq n \leq 8$. The form of the error probability $P_{e,s}$ is

$$P_{e,s} = 1 - \sum_{i=0}^{n-1} a_i P_s^i (1-P_s)^{n-i} \quad (3.55)$$

where a_i are constants that depend on M , the symbol size and P_s is the uncoded symbol error probability.

As mentioned previously we can also use binary codes with M-ary modulation. We do this by treating each M-ary symbol as $\log_2 M$ bits and encoding each bit separately. The uncoded bit error probability $\bar{P}_b$ is given by

$$\bar{P}_b = \frac{1}{2} \frac{M}{M-1} \bar{P}_s \quad (3.56)$$

Now the channel is a BSC with crossover probability $\bar{P}_b$. The bit error probability for binary convolutional codes can be evaluated using the first several terms in (2.40) and using (2.44). The w_j are tabulated in [9] Appendix B for some convolutional codes.

Now consider the case of hard decisions, no memory ($m=1$) and side information available. For this case consider the repetition code with M-ary modulation. If just one symbol in a codeword is not jammed then the decoder decides the transmitted symbol was the symbol received with no jamming. The error probability in this case is zero since there is no noise in the unjammed channels. Thus for an error to occur all n symbols of the repetition code must be jammed. If the jammer is a partial-band jammer then the probability of n symbols being jammed is ρ^n . The symbol error probability for this code is

$$P_{e,s} = \max_{0 \leq \rho \leq 1} \left\{ \rho^n \left[1 - \sum_{i=0}^{n-1} a_i P_s(E_p/N_J)^i (1 - P_s(E_p/N_J))^{n-i} \right] \right\} \quad (3.57)$$

where $P_s(\cdot)$ is given in (3.26). This maximum has the form

$$P_{e,s} = \begin{cases} 1 - \sum_{i=0}^{n-1} a_i P_s^i(E/N_J) (1 - P_s(E/N_J))^{n-i} & E/N_J < A_{M,n} \\ B_{M,n} / (E/N_J)^n & E/N_J \geq A_{M,n} \end{cases} \quad (3.58)$$

for some constants $A_{M,n}$ and $B_{M,n}$. The bit error probability can be calculated using (3.52).

The performance of the repetition code with soft decisions and side information available can also be computed. As with hard decisions, the jammer is forced to jam all symbols in a codeword of a repetition code for an error to occur. The symbol error probability can be computed as

$$P_s^{(n)}(E/N_J) = \max_{0 \leq \rho \leq 1} \{ \rho^n P_s(n\rho E/N_J) \} \quad (3.59)$$

where $P_s(\cdot)$ is given in (3.26). The maximum has the form

$$P_s^{(n)}(E/N_J) = \begin{cases} P_s(nE/N_J) & E/N_J < \varphi_{M,n} \\ \frac{\psi_{M,n}}{(E/N_J)^n} & E/N_J \geq \varphi_{M,n} \end{cases} \quad (3.60)$$

where $\varphi_{M,n}$ and $\psi_{M,n}$ are constants.

For BPSK with memory $m = 1$ we can use binary convolutional codes or repetition codes. The error probability for cases of hard decisions with and without side information are calculated in the same way as for M-ary orthogonal modulation so we do not repeat the calculations.

With BPSK and memory $m > 1$ we consider coding using codes with symbols size larger than 2. The method we use to exploit the channel's memory is to treat each m bit as one symbol in a code.

The probability of a code symbol being in error for partial-band jamming with BPSK is given by

$$P_s = \max_{0 \leq \rho \leq 1} \rho [1 - (1 - Q(\sqrt{2E\rho/N_J}))^m]$$

$$= \begin{cases} 1 - (1 - Q(\sqrt{2E/N_J}))^m & E/N_J < Z_m \\ \frac{W_m}{E/N_J} & E/N_J \geq Z_m \end{cases} \quad (3.61)$$

with W_m and Z_m given in Table 3.4.

Table 3.4. Constants used in computing symbol error probabilities in (3.61).

m	W_m	Z_m	$Q(\sqrt{2Z_m})$
1	0.0828	0.7088	.1169
2	0.1565	0.7633	.1083
3	0.2225	0.8139	.1010
4	0.2827	0.8608	.0947
5	0.3379	0.9048	.0897
6	0.3890	0.9460	.0845
7	0.4365	0.9849	.0802
8	0.4809	1.0218	.0767

The decoded symbol error probability can be computed for R-S codes by using (3.61) in (2.42). The decoded bit error probability $P_{e,b}$ is then given by

$$P_{e,b} = \begin{cases} \frac{Q(\sqrt{2E/N_J})}{1-(1-Q(\sqrt{2E/N_J}))^m} P_{e,s} & E/N_J < Z_m \\ \frac{Q(\sqrt{2Z_m})}{1-(1-Q(\sqrt{2Z_m}))^m} P_{e,s} & E/N_J \geq Z_m \end{cases} \quad (3.62)$$

We now give some numerical results to indicate the improvement obtained by using codes on channels with partial-band jamming. We will be interested in the average bit error probability $P_{e,b}$ for a specific code or equivalently the E_b/N_J necessary to obtain a certain bit error rate. Also of interest is the worst case partial-band jamming strategy ρ^* . Since larger ρ^* means the jammer's optimum strategy is to jam a larger band this might be a costly strategy.

First we give numerical results for the channel without side information and hard decisions. We give results for $M = 32$ (32-ary orthogonal signaling).

In Table 3.5 the E_b/N_J necessary for bit error probability 10^{-3} and 10^{-5} are shown for the length 31 R-S codes when used on this channel. Also shown is the fraction ρ^* of the band for the worst case partial-band jamming strategy. For 10^{-5} error probability the (31,11) RS code requires least energy E_b while for 10^{-3} error probability the (31,13) code requires least energy. The improvement in performance obtained by the (31,11) code in comparison to an uncoded system is 35.1 dB at $P_{e,b} = 10^{-5}$.

The dual k codes performance on the channel with hard decisions, no side information and partial-band jamming is shown in Table 3.6. The rate of the code is $1/v$. The complexity of decoding these codes in terms of storage is proportional to 2^k and is nearly independent of v . Notice that

Table 3.5. Performance of length 31 R-S codes on channel with hard decisions, no side information and partial-band jamming (32-ary orthogonal signaling, bounded distance decoding).

Code	$P_{e,b} = 10^{-3}$		$P_{e,b} = 10^{-5}$	
	E_b/N_J (dB)	ρ^*	E_b/N_J (dB)	ρ^*
No Coding	20.50	0.005	40.50	0.00005
(31,29)	14.35	0.021	24.57	0.002
(31,27)	11.32	0.046	18.37	0.009
(31,25)	9.43	0.076	14.58	0.022
(31,23)	8.16	0.111	12.68	0.039
(31,21)	7.26	0.150	11.13	0.061
(31,19)	6.62	0.196	10.02	0.088
(31,17)	6.19	0.237	9.23	0.118
(31,15)	5.95	0.283	8.70	0.151
(31,13)	5.84	0.335	8.38	0.187
(31,11)	5.94	0.388	8.27	0.226
(31,9)	6.26	0.442	8.41	0.268
(31,7)	6.82	0.497	8.83	0.313
(31,5)	7.79	0.557	9.68	0.360
(31,3)	9.95	0.618	11.34	0.410
(31,1)	13.90	0.681	15.56	0.464

Table 3.6. Performance of dual-5 codes on channel with hard decisions, no side information and partial-band jamming (32-ary orthogonal signaling).

v	E_b/N_J (dB)	$P_{e,b} < 10^{-3}$	E_b/N_J (dB)	$P_{e,b} < 10^{-5}$
		ρ^*		ρ^*
1 (No Coding)	20.50	0.005	40.50	0.00005
2	12.95	0.055	20.22	0.010
3	8.93	0.207	13.32	0.075
4	7.53	0.381	10.79	0.180
5	6.97	0.542	9.44	0.307
6	6.75	0.684	8.79	0.428
7	6.71	0.806	8.44	0.541
8	6.75	0.912	8.27	0.643
9	6.85	1.000	8.20	0.736
10	6.95	1.000	8.19	0.819
11	7.05	1.000	8.22	0.895
12	7.13	1.000	8.29	0.963
13	7.22	1.000	8.35	1.000
14	7.29	1.000	8.43	1.000
15	7.36	1.000	8.49	1.000

for small enough rates, the worst case of partial-band jamming strategy is in fact uniform jamming ($\rho^* = 1.0$). An identical conclusion was obtained from capacity and cutoff rate considerations.

Let us now compare the performance of the dual-k and R-S codes. In comparing two codes we must keep the code rates the same. For example the dual-5 code with rate $\frac{1}{2}$ ($r = 2$) requires $E_b/N_J = 20.22$ dB for error probability 10^{-5} . The (31,15) R-S code with rate $\approx \frac{1}{2}$ requires only 8.7 dB. The rate $\frac{1}{3}$ ($r = 3$) dual-5 code requires $E_b/N_J = 13.32$ dB for error probability 10^{-5} while the (31,11) R-S code requires only 8.27 dB. The rate $\frac{1}{10}$ dual-5 code requires $E_b/N_J = 9.19$ dB while the (31,3) requires 11.34 dB. The comparisons made include not only the code under consideration but also the decoding algorithm. The performance of the dual-k code was computed assuming maximum likelihood decoding (Viterbi decoding) while the performance of the R-S code was computed using bounded distance decoding. For high code rates bounded distance decoding is nearly maximum likelihood. However, for low code rates this is not the case. For example the (31,1) R-S code is actually just a repetition code of length 31 and is capable of correcting some patterns of 29 errors with maximum likelihood decoding. The bounded distance decoder only corrects 15 errors and no more. Thus, on the channel with hard decisions, partial-band jamming and no side information, for low code rates ($< 1/8$) R-S codes with bounded distance decoding become inferior to dual-k codes because of the decoding algorithm. For moderately large rates ($> 1/3$) R-S codes with bounded distance decoding are superior to dual-k codes with Viterbi decoding.

For comparison purposes we can bound the bit error probability for R-S codes with maximum likelihood decoding (MLD) by using the union bound [9, eqns. (1-28) and (2-22)]. The performance of the (31,5), (31,3), and (31,1) codes are shown in Table 3.8. As can be seen the optimal duty factor ρ^* is larger when using MLD than for bounded distance decoding. Although MLD is not currently being implemented we shall see later that by combining a repetition code with a R-S code with bounded distance decoding forces the duty factor to one.

The performance of binary convolutional codes with Viterbi decoding (MLD) on the 32-ary channel using separate codes on each of the 5 bits in a 32-ary symbol can be calculated using (3.56), (3.29), (2.40) and (2.44) with $\epsilon = \bar{P}_b$. We consider the rate $\frac{1}{2}$ constraint length 7 and 9 convolutional codes in [9, Appendix B]. In Table 3.9 we indicate the performance of these codes. Notice that these codes are inferior to the (31,15) RS code with bounded distance decoding. Part of the reason for this is that binary convolutional codes with 32-ary signaling are in effect interleaving and so when side information is not present this interleaving degrades the performance. Massey [23] considered using binary convolutional codes on the M-ary pulse position modulation photon channel. That channel fits the models of chapter 2 and has side information available intrinsically. Massey found that convolutional codes on the photon channel has performance comparable to the R-S codes. We attribute this to the fact that side information was available. Without side information R-S codes outperform convolutional codes.

Table 3.7. Performance of R-S codes on channel with hard decisions,
no side information, and partial-band jamming
(32-ary orthogonal signaling, maximum likelihood decoding).

Code	$P_{e,b} < 10^{-3}$		$P_{e,b} < 10^{-5}$	
	$E_b/N_J(\text{dB})$	ρ^*	$E_b/N_J(\text{dB})$	ρ^*
(31,5)	6.89	0.684	7.81	0.586
(31,3)	7.71	0.945	8.60	0.771
(31,1)	10.61	1.000	11.76	1.000

Table 3.8. Performance of binary convolutional codes on channel
with hard decisions, no side information and partial-
band jamming (32-ary orthogonal signaling, Viterbi
decoding).

Code	$P_{e,b} < 10^{-3}$		$P_{e,b} < 10^{-5}$	
	$E_b/N_J(\text{dB})$	ρ^*	$E_b/N_J(\text{dB})$	ρ^*
K=7	8.00	0.171	11.21	0.082
K=9	6.44	0.245	9.36	0.125

We consider now repetition codes on the channel with and without side information with hard decisions for the former case and with both hard and soft decisions for the latter case. The case of 32-ary orthogonal signaling and BPSK are examined. The symbol error probability for hard decisions without side information is given in (3.55) with $P_s = \bar{P}_s(E/N_J)$ given in (3.29). In Table 3.9 the performance of repetition codes of length $3 \leq n \leq 8$ is shown.

Table 3.9. Performance of length n , rate $1/n$ repetition codes on channel with hard decisions, no side information and partial-band jamming (32-ary orthogonal signaling).

n	$P_{e,b} = 10^{-3}$		$P_{e,b} = 10^{-5}$	
	E_b/N_J (dB)	ρ^*	E_b/N_J (dB)	ρ^*
3	13.21	0.077	23.24	0.0077
4	10.43	0.196	18.55	0.0301
5	9.18	0.326	15.28	0.080
6	8.57	0.451	13.50	0.145
7	8.26	0.564	12.40	0.217
8	8.12	0.666	11.69	0.293

The performance of repetition codes on the channel with side information, hard decisions and partial-band jamming is shown in Table 3.10. In Table 3.11 the corresponding results are shown for soft decisions. Note that soft decisions can improve the performance by between 3 and 4 dB.

Table 3.10. Performance of repetition codes on channel with side information, hard decisions and partial-band jamming (32-ary orthogonal signaling).

Code	$P_{e,b} = 10^{-3}$		$P_{e,b} = 10^{-5}$	
	E_b/N_J (dB)	ρ^*	E_b/N_J (dB)	ρ^*
(3,1)	9.58	0.264	16.25	0.057
(4,1)	8.36	0.438	13.36	0.139
(5,1)	7.86	0.604	11.86	0.240
(6,1)	7.70	0.748	11.04	0.347
(7,1)	7.71	0.868	10.56	0.449
(8,1)	7.79	0.966	10.29	0.543

Table 3.11. Performance of repetition codes on channel with side information, soft decisions and partial-band jamming.

Code	$P_{e,b} = 10^{-3}$		$P_{e,b} = 10^{-5}$	
	E_b/N_J (dB)	ρ^*	E_b/N_J (dB)	ρ^*
(3,1)	6.59	0.381	13.25	0.063
(4,1)	5.39	0.493	10.39	0.156
(5,1)	4.87	0.677	8.87	0.269
(6,1)	4.64	0.838	7.98	0.389
(7,1)	4.58	0.978	7.44	0.507
(8,1)	4.58	1.000	7.10	0.619

We plot in Figures 3.13-3.15 the symbol error probability for repetition codes of length 1,3,5, and 7 for the cases of i) hard decisions, no side information, ii) hard decisions with side information, iii) soft decisions with side information. Notice that with hard decisions there is an optimal diversity or code length such that for fixed E_b/N_J the symbol error probability is minimized. For soft decisions with side information however, the symbol error probability decreases as the diversity increases. We will see in the next chapter that this is not true when there is noncoherent demodulation and soft decisions. Notice also that for soft decisions with n large the optimum duty factor is one so that partial-band jammers are neutralized.

These repetition codes can also be concatenated with Reed-Solomon codes. In Tables 3.12-3.15 the performance of R-S codes when used in conjunction with repetition codes is shown. The R-S codes were chosen for each diversity to E_b/N_J for bit error probability 10^{-3} .

Code	E_b/N_J (dB)	$P_{e,b}=10^{-3}$	ρ^*
(3,1)(31,17)	7.12		0.513
(4,1)(31,21)	6.57		0.702
(5,1)(31,21)	6.48		0.895
(6,1)(31,21)	6.61		0.968
(7,1)(31,23)	6.70		1.000

Table 3.12. Performance of repetition codes and R-S code on channel with hard decisions and no side information (32-ary orthogonal signaling).

Table 3.13. Performance of repetition codes and R-S code on channel with hard decisions and side information (32-ary orthogonal signaling).

Code	$P_{e,b}=10^{-3}$	
	E_b/N_J (dB)	ρ^*
(3,1)(31,17)	6.55	0.966
(4,1)(31,21)	6.31	1.000
(5,1)(31,21)	6.45	1.000
(6,1)(31,21)	6.61	1.000
(7,1)(31,23)	6.69	1.000

Table 3.14. Performance of repetition codes and R-S codes on channel with soft decisions and side information (32-ary orthogonal signaling).

Code	$P_{e,b}=10^{-3}$	
	E_b/N_J (dB)	ρ^*
(3,1)(31,17)	3.54	1.000
(4,1)(31,21)	3.28	1.000
(5,1)(31,21)	3.28	1.000
(6,1)(31,21)	3.28	1.000
(7,1)(31,23)	3.26	1.000

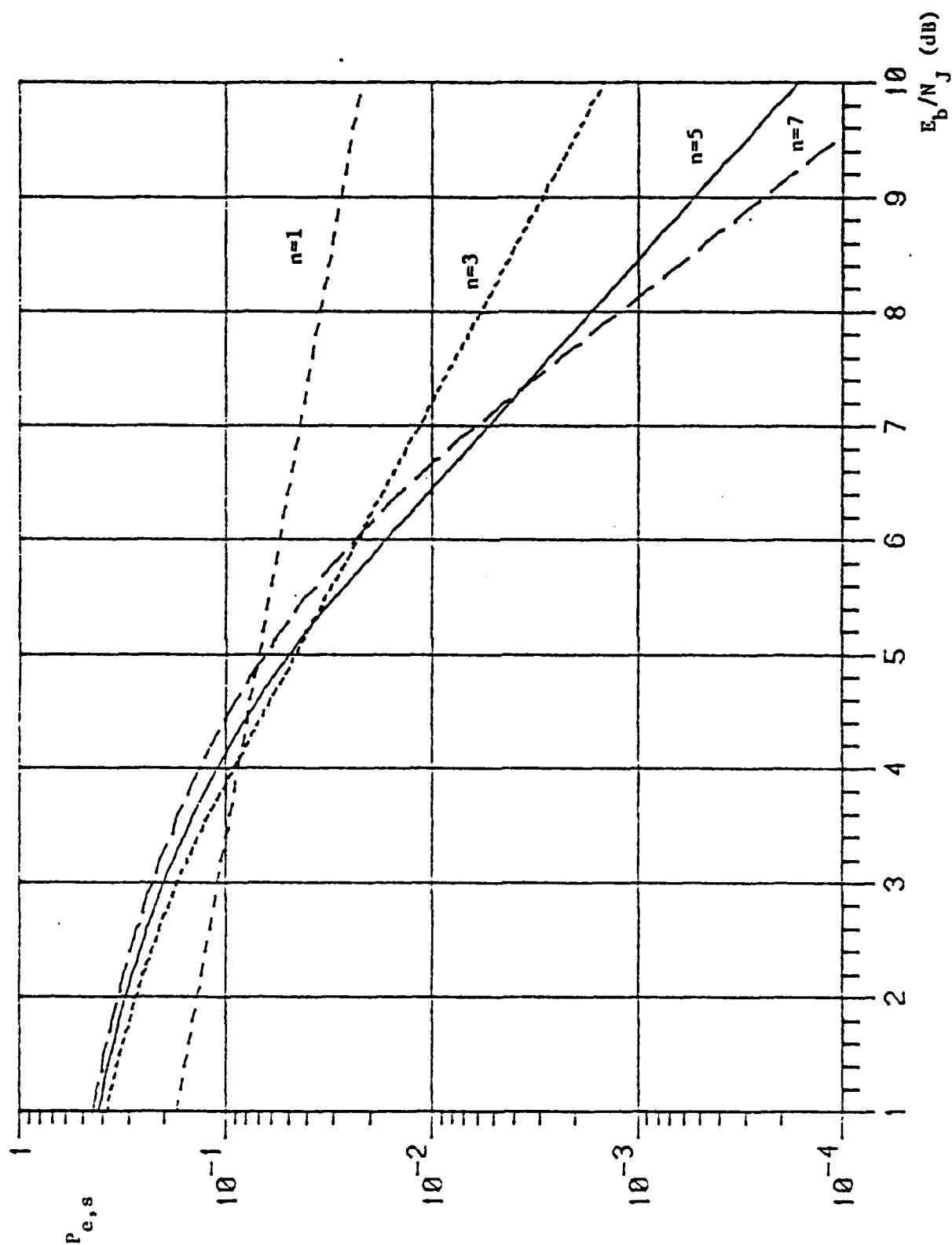


Figure 3.13. Symbol error probability for repetition codes on channel with hard decisions and no side information (32-ary orthogonal signaling).

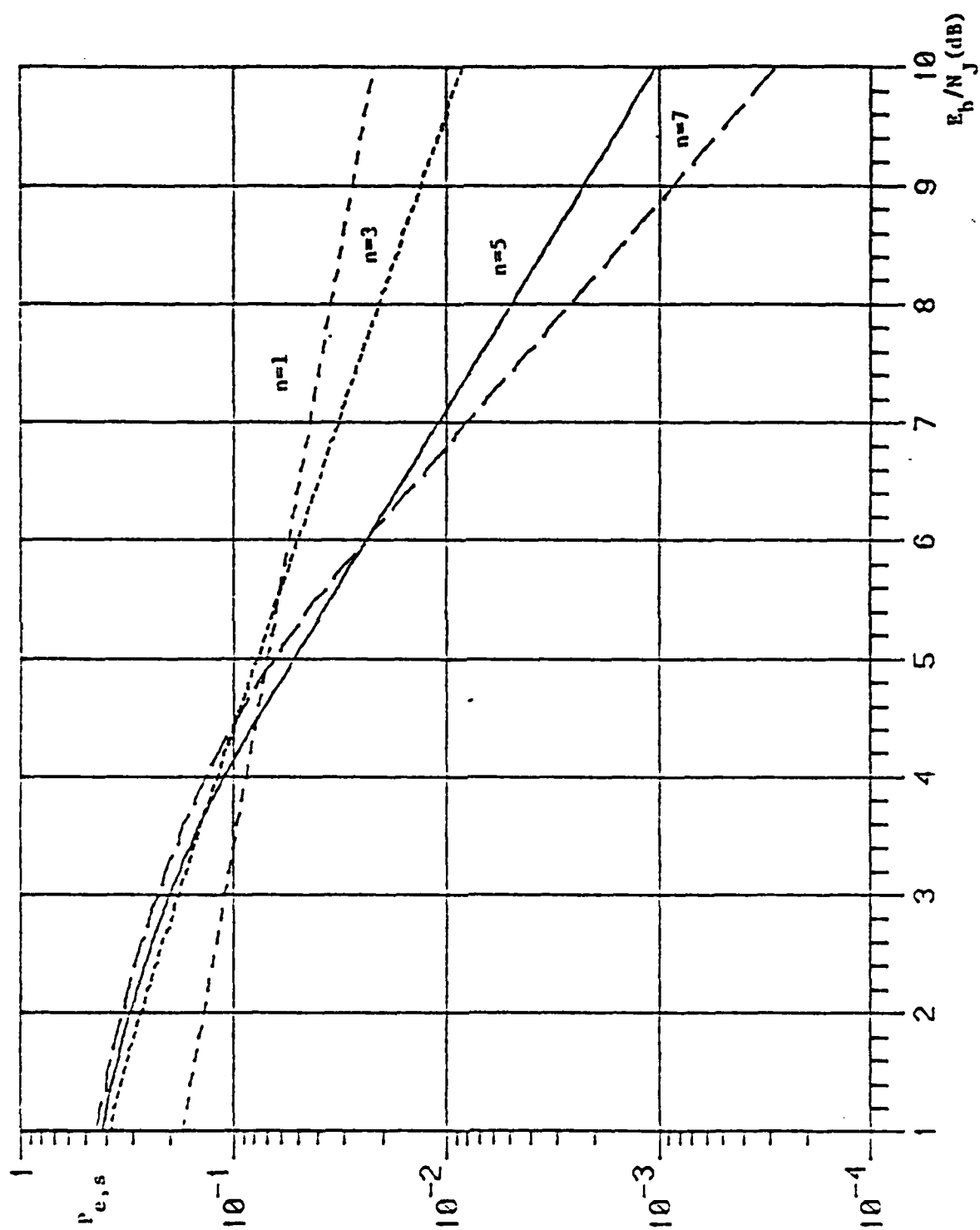


Figure 3.14. Symbol error probability for repetition codes on channel with hard decisions and side information available (32-ary orthogonal signaling).

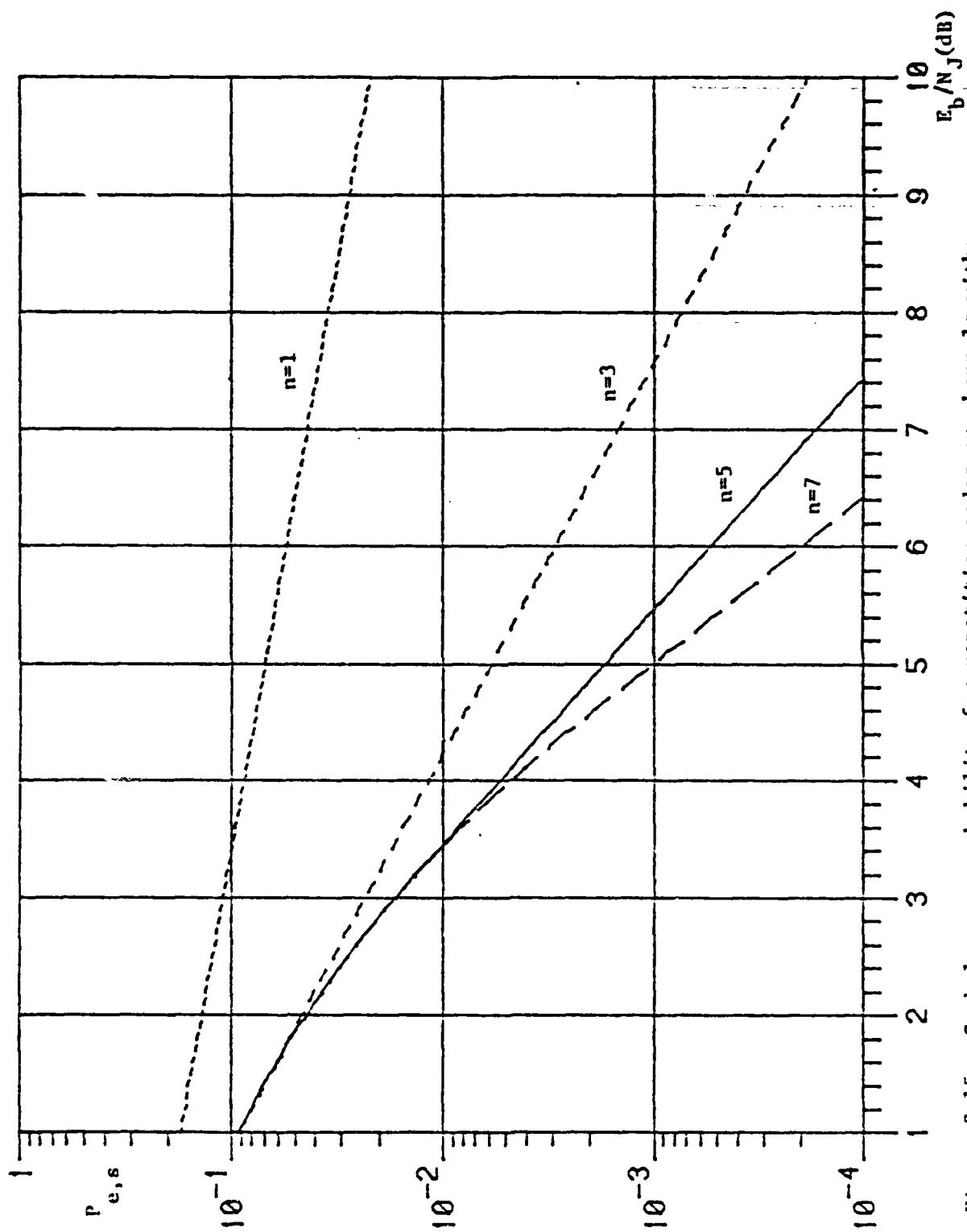


Figure 3.15. Symbol error probability for repetition codes on channels with soft decisions and side information available (32-ary orthogonal signaling).

So far we have only considered the case of memory $m = 1$ (i.e. memoryless). The case of memory $m > 1$ can most easily be examined by considering BPSK with hard decisions and no side information. The symbol error probability for a symbol consisting of m bits may be calculated in (3.61). If we use R-S codes of length $2^m - 1$ then the decoded symbol error probability can be calculated using (2.38). The bit error probability is found by using (3.62). In Figure 3.16 the bit error probability for the (31,15) and (255,127) RS codes is plotted versus E_b/N_J computed using (3.31a) with $M = 2$. The performance of the constraint length 7 and 9, rate $\frac{1}{2}$ binary convolutional codes given in [9, Appendix B] with full interleaving ($m = 1$) is also shown.

Note that when the jammer is present for a particular symbol the uncoded bit error probability is $Q(\sqrt{2Z_m})$ independent of the signal-to-noise ratio E/N_J . For $m = 5$, $Q(\sqrt{2Z_m}) = 0.0892$ while for $m = 8$, $Q(\sqrt{2Z_m}) = 0.0764$. From Figure 3.16 we see that the convolutional codes perform much better on this channel relative to the R-S codes than on the channel of Chapter 2. This is due to the fact that the bit error rate when the jammer is on is very low (compared to $\frac{1}{2}$). Although we expect interleaving to hurt the performance relative to uninterleaved systems, the memory here is not very dominant. In the example of Chapter 2 the error probability is $\frac{1}{2}$ when the jammer is on so that the expected number of bit errors is just $\frac{1}{2} m$ or 2.5 for $m = 5$, and 4 for $m = 8$. While for the above channel the expected number of bit errors in a symbol is 0.446 for $m = 5$ and 0.611 for $m = 8$ so that most symbol errors are caused by single bit errors.

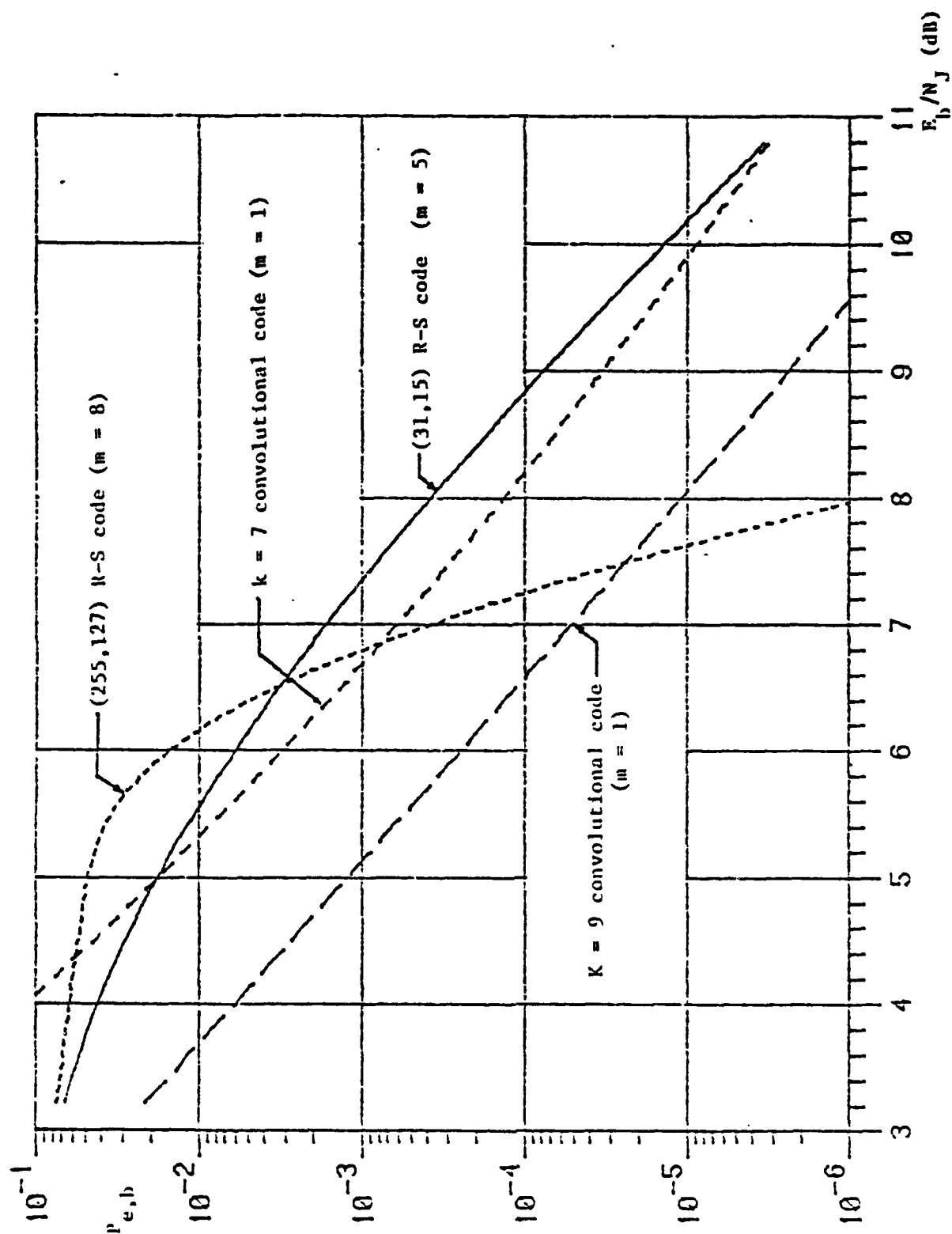


Figure 3.16. Bit error probability for BPSK with hard decisions, with and without memory.

CHAPTER 4

CODING FOR CHANNELS WITH PARTIAL-BAND JAMMING AND NONCOHERENT DEMODULATION

4.1 Introduction

In this chapter we examine the performance of frequency-hopped spread-spectrum communication system subject to partial-band jamming with noncoherent demodulation. We consider M-ary orthogonal signals with frequency shift keying on multiple frequency shift keying (MFSK). The modulated signal is frequency hopped to produce the transmitted signal. The received signal is dehopped and then demodulated to produce the channel output. The jammer adds noise to the signal only over a fraction of the frequency band the transmitter is using. The strategy of the jammer corresponds to the fraction of the band that is jammed. We will consider the performance for the worst case jamming strategy.

The remainder of the chapter is divided into four sections. In Section 4.2 the channel models will be described for MFSK with noncoherent demodulation. We will consider the MFSK for M-ary orthogonal signals to simplify the description. The capacity for the channel described in Section 4.2 is computed in Section 4.3 with and without side information available at the channel output. In Section 4.4 we repeat the calculations for the cutoff rate. In Section 4.5 the performance of specific codes is evaluated when side information is and is not available. We compare the coded performance to the channel capacity and cutoff rate.

4.2 Channel Models

In this section the channel models for frequency-hopped spread-spectrum communication using MFSK are given when there is partial-band jamming. As mentioned in Chapter 1 we treat the frequency hopper and dehopper as performing inverse operations on the modulated signal. The output of the frequency dehopper consists of two additive terms. The first term corresponds to the received signal in the absence of noise, while the second term is due to the jammer's signal. This second term is nonzero only if there was a jamming signal in the band that the MFSK signal was transmitted in. This band includes the frequencies of all possible MFSK signals the modulator produces.

Consider frequency hopping with m symbols per hop. Since as in Chapter 3 we assume the channel is memoryless from hop to hop describing the channel for a single hop is sufficient to describe the channel. For MFSK the input alphabet $A = \{0, 1, \dots, M-1\}$. Assume that the particular hop begins at time $t = 0$ and is of duration mT where T is the duration of one MFSK signal. When the input X_j , $0 \leq j < m$, takes the value $i \in A$, the data modulated signal $\hat{s}_i(t-jT)$ is the input to the frequency hopper during the interval $jT \leq t \leq (j+1)T$. The signal $\hat{s}_i(t)$ is given by

$$\hat{s}_i(t) = \sqrt{2P} \cos(\omega_i t + \theta_i) p_T(t) \quad (j-1)T \leq t < jT \quad (4.1)$$

where ω_i , $0 \leq i \leq M$, is the radian frequency of the signal, P is the power and T is the duration. (We assume throughout that $\{\hat{s}_i(t)\}_{i \in A}$ forms an orthogonal signal set.) In (4.1) θ_i , $0 \leq i \leq M-1$ is the phase of the i -th signal. The frequency hopper changes the center frequency of the modulated signal in different hops to one of q different center frequencies according

to a specified hopping to produce the transmitted signal $s_i(t-jT)$ during the interval $jT \leq t < (j+1)T$, $0 \leq j < m$, given by

$$s_i(t) = \sqrt{2P} p_T(t) \cos(\omega_\ell + \omega_i)t + \varphi_i) \quad (4.2)$$

where ω_ℓ $1 \leq \ell \leq q$ are the q different center frequencies of the hopping pattern.

The model for the jamming signal is the same as in Chapter 3 so we do not repeat the descriptions here.

The received signal $r(t)$ when $s_i(t-jT)$, $0 \leq j < m$, is transmitted consists of the sum of the transmitted signal and the jamming signal:

$$r(t) = s_i(t-jT) + j(t), \quad jT \leq t \leq (j+1)T \quad (4.3)$$

(Here we assume without loss of generality that all time delays are zero.) The frequency dehopper changes the center frequency of the received signal according to the hopping pattern of the transmitter. A possible random phase shift is also introduced. The signal $\hat{r}(t)$ at the output of the frequency dehopper is then given by

$$\hat{r}(t) = \sqrt{2P} \cos(\omega_i t + \varphi_i) p_T(t) + \hat{j}_\ell(t) \quad (j-1)T \leq t < jT \quad (4.4)$$

where $\hat{j}_\ell(t)$ is the bandpass process obtained from when $j(t)$ is frequency translated by $-\omega_\ell$ and then filtered by an ideal bandpass filter with center frequency ω_i and bandwidth $2\omega_L$. The bandwidth ω_L is chosen large enough so that each of the MFSK signals is essentially unaltered when filtered by this bandpass filter. Also in (4.4) φ_i is a random phase which accounts for the phase introduced by the frequency hopper, dehopper, and any transmission delays.

AD-A125 872

CODING FOR FREQUENCY-HOPPED SPREAD-SPECTRUM CHANNELS
WITH PARTIAL-BAND INTERFERENCE(U) ILLINOIS UNIV AT
URBANA COORDINATED SCIENCE LAB W E STARK JUL 82 R-945

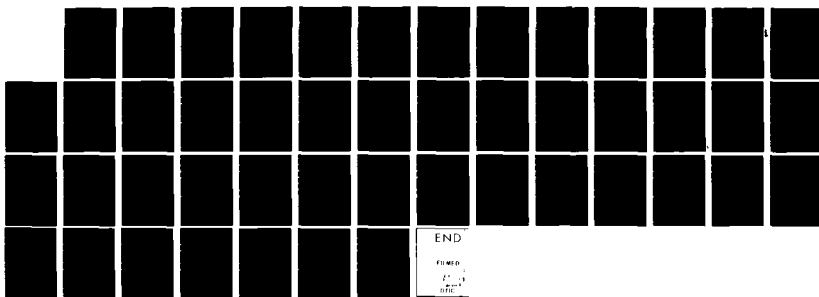
2/2

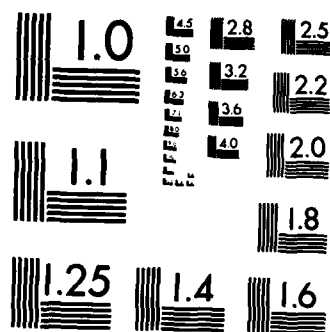
UNCLASSIFIED

N00014-79-C-0424

F/G 17/2

NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

The demodulator we consider processes the received signal $\hat{r}(t)$ by computing the M-dimensional vector $\underline{y}^{(j)} = (y_{1,j}, y_{2,j}, \dots, y_{M-1,j})$ where

$$y_{i,j} = \left(\frac{4}{N_J T} \right)^{\frac{1}{2}} \left[\left(\int_{(j-1)T}^{jT} \hat{r}(t) \cos \omega_1 t dt \right)^2 + \left(\int_{(j-1)T}^{jT} \hat{r}(t) \sin \omega_1 t dt \right)^2 \right],$$

$$0 \leq i \leq M-1 \quad (4.5)$$

The density $p(y_{k,j} | X=i, Z=1/\rho)$ of $y_{k,j}$ given $X_j = i$ and the jammer is on can be shown to be given by

$$p(y_{k,j} | X=i, Z=1/\rho) = \begin{cases} y_{k,j} \exp\{-\frac{1}{2}(y_{k,j}^2 + \beta^2)\} I_0(\beta y_{k,j}) & , \quad k = i \\ y_{k,j} \exp\{-\frac{1}{2} y_{k,j}^2\} & , \quad k \neq i \end{cases} \quad (4.6)$$

where $\beta = 2PT/N_J Z = 2 E/N_J Z$ and β_T is defined as the energy per transmitted symbol. When the jammer is off ($Z=0$) we have

$$P\{y_{i,j} = \sqrt{2 E/N_J} \delta_{i,k} | X_j = i, Z = 0\} = 1 \quad (4.7)$$

where $\delta_{i,k}$ is 1 for $k = i$ and zero otherwise.

Note that the receiver can tell given $y_{k,j}$ whether or not the jammer was on during the hop by checking if $y_{k,j} = \sqrt{2 E/N_J} \delta_{i,k}$ for some i so that side information is available. However, the receiver might just decide that s_i was transmitted in $[(j-1)T, jT]$ if $y_{i,j} > y_{k,j}$ $k \neq i$. In this case the receiver makes a hard decision and disregards the side information. Alternatively the receiver may know which hops were jammed and make hard decisions. In the next section we compute the capacity of the partial-band noise jamming channel for the cases stated above.

4.3 Channel Capacity

In this section we derive expressions for the capacity of frequency hopped MFSK with partial-band jamming. We compare this to the capacity when the jammer corrupts the entire frequency band of the system ($\rho = 1$). We conclude that provided codes of rate smaller than some critical rate are used, $\rho = 1$ is the worst case partial-band jamming threat.

We treat the case of the receiver having side information first. When the jammer is on the channel is a M-ary FSK additive Gaussian noise channel with signal energy-to-noise ratio $2E_p/N_J$. The capacity $C_M(E_p/N_J)$ of this component channel is achieved with a uniform input distribution on A. When the jammer is off the component channel is a M-ary symmetric channel with error probability zero and capacity (measured in M-ary symbols per channel use) equal to 1.0. Thus both component channels have the same input distribution that achieves capacity. In this case from (2.18) the capacity of the composite channel is independent of the memory length m of the channel. The capacity $\bar{C}(E/N_J)$ for M-ary FSK with worst case partial-band jamming is given by

$$\bar{C}_M(E/N_J) = \min_{0 \leq \rho \leq 1} \{ \rho C_M(E_p/N_J) + (1 - \rho) \} \quad (4.8)$$

The minimum in (4.8) can be found numerically or by setting the first derivative equal to zero:

$$\frac{\partial}{\partial \rho} \{ \rho C_M(E_p/N_J) + (1 - \rho) \} = 0$$

or

$$C_M(E_p/N_J) + E_p/N_J C'_M(E_p/N_J) = 1 \quad (4.9)$$

where $C'(x) = \partial C(x)/\partial x$. From (4.9) we can determine the dependence of the worst case $\rho = \rho^*$ on the signal-to-noise ratio E/N_J as

$$\rho^* = \begin{cases} 1 & E/N_J < \gamma_M \\ \frac{\gamma_M}{E/N_J} & E/N_J \geq \gamma_M \end{cases} \quad (4.10)$$

where γ_M is the solution of

$$C_M(\gamma_M) + \gamma_M C'_M(\gamma_M) = 1 \quad (4.11)$$

Using (4.10) in (4.8) we obtain

$$\bar{C}_M(E/N_J) = \begin{cases} C_M(E/N_J) & E/N_J < \gamma_M \\ 1 - \frac{\gamma_M - \gamma_M C_M(\gamma_M)}{E/N_J} & E/N_J \geq \gamma_M \end{cases} \quad (4.12)$$

If codes of rate r (measured in M -ary units) are used then reliable communication is possible provided $r < \bar{C}(E/N_J)$ (see Theorem 2, Chapter 2).

In the case $E/N_J > \gamma_M$ reliable communication is possible provided

$$r < 1 - \frac{\gamma_M - \gamma_M C_M(\gamma_M)}{E/N_J}$$

or

$$E/N_J > \frac{\gamma_M - \gamma_M C_M(\gamma_M)}{(1-r)} = \frac{\gamma_M (1 - C_M(\gamma_M))}{(1-r)} \quad (4.13)$$

Since E is the energy per transmitted signal and $\log_2 M$ bits are transmitted per signal the energy per information bit with code of rate r is

$$E_b/N_J = (E/N_J)/r \log_2 M$$

so that (4.13) becomes

$$E_b/N_J > \frac{\gamma_M(1-C_M(\gamma_M))}{\log_2 M(1-r)r} \quad (4.14)$$

We wish to choose the code rate that minimizes the right hand side of (4.14). The minimum can easily be shown to occur at $r = r^* = \frac{1}{2}$. Thus for the optimal code rate we need

$$E_b/N_J > \frac{4\gamma_M(1-C_M(\gamma_M))}{\log_2 M} \quad (4.15)$$

This holds provided $E/N_J > \gamma_M$ or equivalently $C_M(\gamma_M) < \frac{1}{2}$. Note that so far we have not specified the type of receiver (e.g. hard decisions, soft decisions). For a particular receiver structure we need only compute $C_M(x)$ and $C'_M(x)$ to solve (4.11). Notice from (4.10) that provided $E/N_J < \gamma_M$ or equivalently $C_M(E/N_J) < \gamma_M$ the worst case partial-band jamming strategy is in fact uniform jamming.

For binary FSK with soft decisions (so side information is available) $C_2(x)$ has been computed [5] as

$$C_2(x) = \exp\{-x^2\} \int_0^\infty \int_0^\infty y_0 y_1 \exp\{-\frac{1}{2}(y_0^2 + y_1^2)\} I_0(2xy) \cdot \log \left\{ \frac{2I_0(2xy_0)}{I_0(2xy_0) + I_0(2xy_1)} \right\} dy_0 dy_1 \quad (4.16)$$

We can also compute $C'_2(x)$ by differentiating (4.15) for soft decisions with binary FSK and partial-band jamming

$$\bar{C}_2(E/N_J) = \begin{cases} C(E/N_J) & E/N_J < 2.4137 \\ 1 - \frac{1.1741}{E/N_J} & E/N_J \geq 2.4137 \end{cases} \quad (4.17)$$

Notice in this case $\gamma_M = 2.4137$ and $C(\gamma_M) = 0.51359 > 0.5$ so that (4.14) is not valid. The optimal code rate in this case can be found numerically to be approximately 0.48.

For M-ary FSK with hard decisions the capacity $\hat{C}_M(x)$ is given by (3.27) with P replaced by $P_s(E/N_J)$ given by

$$P_s(E/N_J) = \frac{1}{M} \sum_{j=2}^M (-1)^j \binom{M}{j} \exp\{-E/N_J(1 - 1/j)\} \quad (4.18)$$

For partial-band jamming with side information available and hard decisions the capacity $\tilde{C}_M(E/N_J)$ can be computed using (4.8)-(4.12) as

$$\tilde{C}_M(E/N_J) = \begin{cases} \hat{C}_M(P_s(E/N_J)) & E/N_J < \tilde{\gamma}_M \\ 1 - \frac{\tilde{\gamma}_M - \tilde{\gamma}_M \tilde{C}_M(P_s(\tilde{\gamma}_M))}{E/N_J} & E/N_J \geq \tilde{\gamma}_M \end{cases} \quad (4.19)$$

where $\tilde{\gamma}_M$ is a constant. In Table 4.1 we list the values of $\tilde{\gamma}_M$ and $\hat{C}_M(\tilde{\gamma}_M)$ for $M = 2, 4, 8, 16$ and 32. Notice that $\hat{C}_M(\tilde{\gamma}_M) < \frac{1}{2}$ so that the optimal code rate for these cases is $r = \frac{1}{2}$.

When side information is not available the capacity depends on the memory length of the channel. For $m = 1$ the channel is a memoryless MSC with symbol error probability given by the average of the error probabilities of the

component channels. Since capacity is a decreasing function of the symbol error probability maximizing symbol error probability is equivalent to minimizing capacity. The maximum of the average error probability $\bar{P}_s(E/N_J)$ has been computed [15] as

$$\bar{P}_s(E/N_J) = \max_{0 \leq \rho \leq 1} \{ \rho P_s(E\rho/N_J) \}$$

$$= \begin{cases} P_s(E/N_J) & E/N_J < \lambda_M \\ \frac{\lambda_M P_s(\lambda_M)}{E/N_J} & E/N_J \geq \lambda_M \end{cases} \quad (4.20)$$

The capacity is found using (3.27) with $P = \bar{P}_s(E/N_J)$ given in (4.20).

Thus the capacity $\bar{C}_M(E/N_J)$ with no side information is given by

$$C_M(E/N_J) = \begin{cases} \hat{C}_M(P_s(E/N_J)) & E/N_J < \lambda_M \\ \hat{C}_M \frac{(\lambda_M P_s(\lambda_M))}{E/N_J} & E/N_J \geq \lambda_M \end{cases} \quad (4.21)$$

The values of λ_M , $P_s(\lambda_M)$ and $C_M(\lambda_M)$ are given in Table 4.1.

Table 4.1. Values of constants used to determine capacity for M-ary FSK.

M	$\tilde{\gamma}_M$	$\bar{C}_M(\gamma_M)$	λ_M	$\bar{P}_s(\lambda_M)$	$C_M(\lambda_M)$
2	3.0169	0.4982	2.0000	0.1839	0.3114
4	3.275	0.4878	2.3830	0.2933	0.3311
8	3.6610	0.4721	2.7821	0.3687	0.3384
16	4.0152	0.4540	3.1924	0.4259	0.3380
32	4.3882	0.4354	3.6132	0.4715	0.3333

To interpret these results we plot the E_b/N_J needed to achieve capacity (see 3.31b).

For soft decisions binary FSK the capacity is given in (4.17). In Figure 4.1 we plot E_b/N_J needed to achieve capacity. This is compared to the E_b/N_J needed to achieve capacity for uniform jamming. For rates less than 0.513 uniform jamming is the optimal partial-band jamming strategy. Notice the increase in E_b/N_J necessary for reliable communications for low rates. This did not happen for BPSK with soft decisions. We explain this increase as the noncoherent combining loss encountered when the receiver does not demodulate the transmitted signal coherently and the code rates are small.

For hard decisions M-ary FSK with and without side information the E_b/N_J needed for reliable communications is shown in Figures 4.2-4.6 for $M = 2, 4, 8, 16$, and 32. The rates below which uniform jamming is optimal are given in Table 4.1. These curves are for the case of $m = 1$. In Figure 4.2 we also plot the E_b/N_J necessary for reliable communication when $m > 1$.

For $m > 1$ the capacity is given by (2.35) with $\epsilon = \rho$ and $\alpha_{m,k}$ given by

$$\alpha_{m,k} = \begin{cases} (1-\rho) + \rho(1-\frac{1}{2}e^{-E_b/2N_J}) & k = 0 \\ \rho(\frac{1}{2}e^{E_b/2N_J})^k(1-\frac{1}{2}e^{-E_b/2N_J})^{m-k} & k = 1, 2, \dots, m \end{cases} \quad (4.22)$$

The minimum in (2.35) no longer has the simple inverse linear relation for the case $m = 1$.

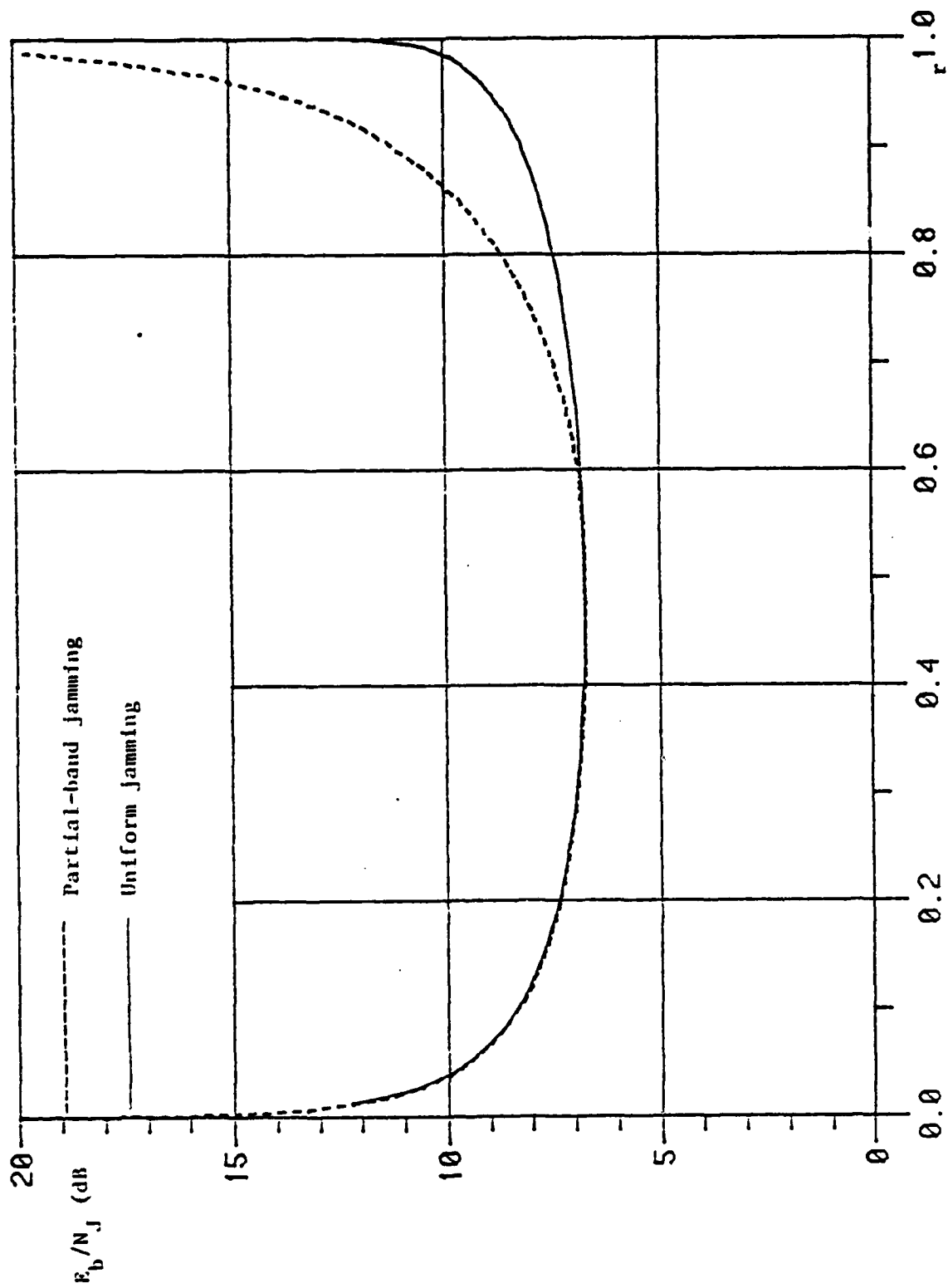


Figure 4.1. E_b/N_j needed to achieve capacity for binary FSK with soft decisions and partial-band jamming (side information available).

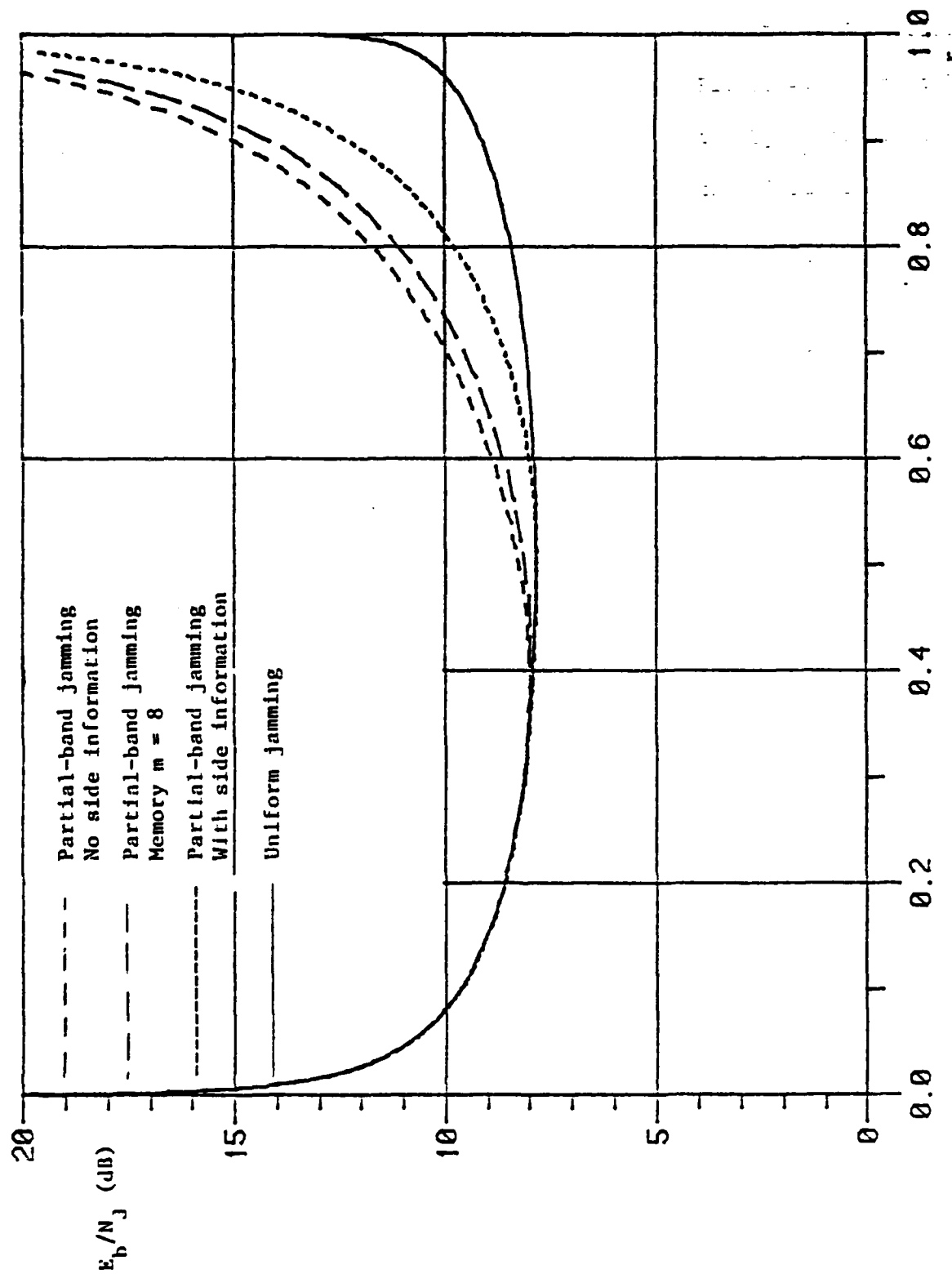


Figure 4.2. E_b/N_j needed to achieve capacity for binary FSK with hard decisions and partial-band jamming.

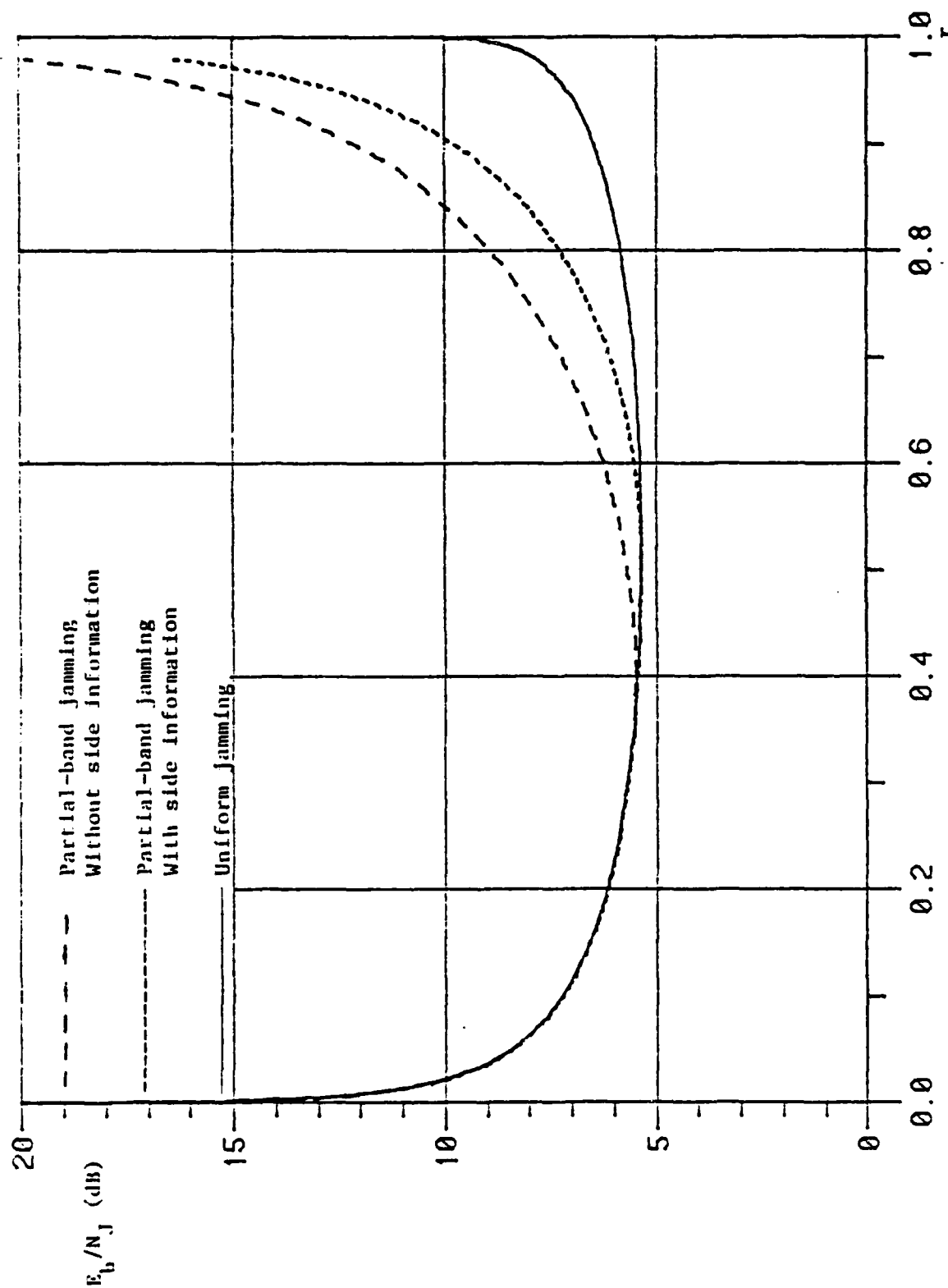


Figure 4.3. E_b/N_j needed to achieve capacity for 4-ary FSK with hard decisions and partial-band jamming.

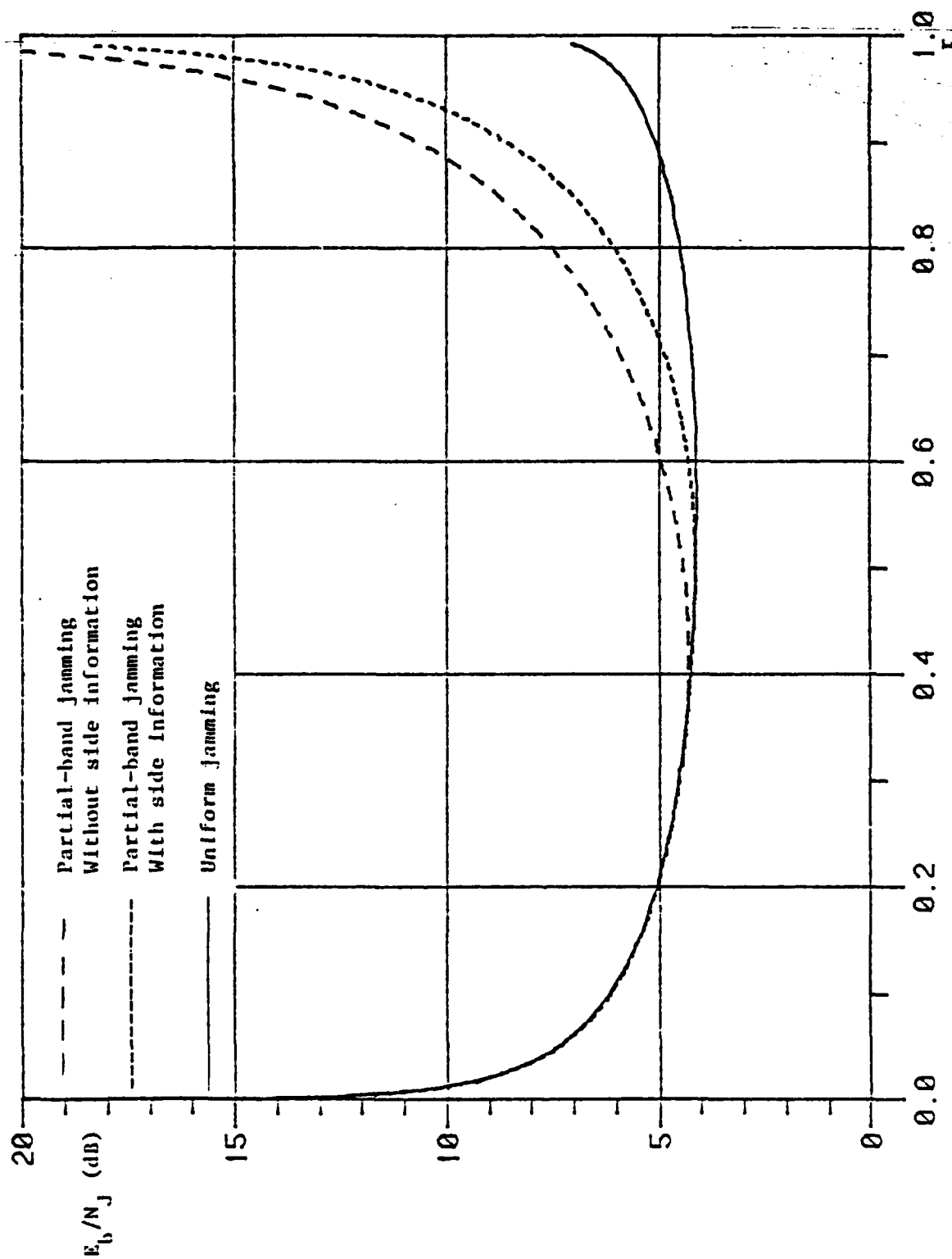


Figure 4.4. E_b/N_J needed to achieve capacity for 8-ary FSK with partial-band jamming.

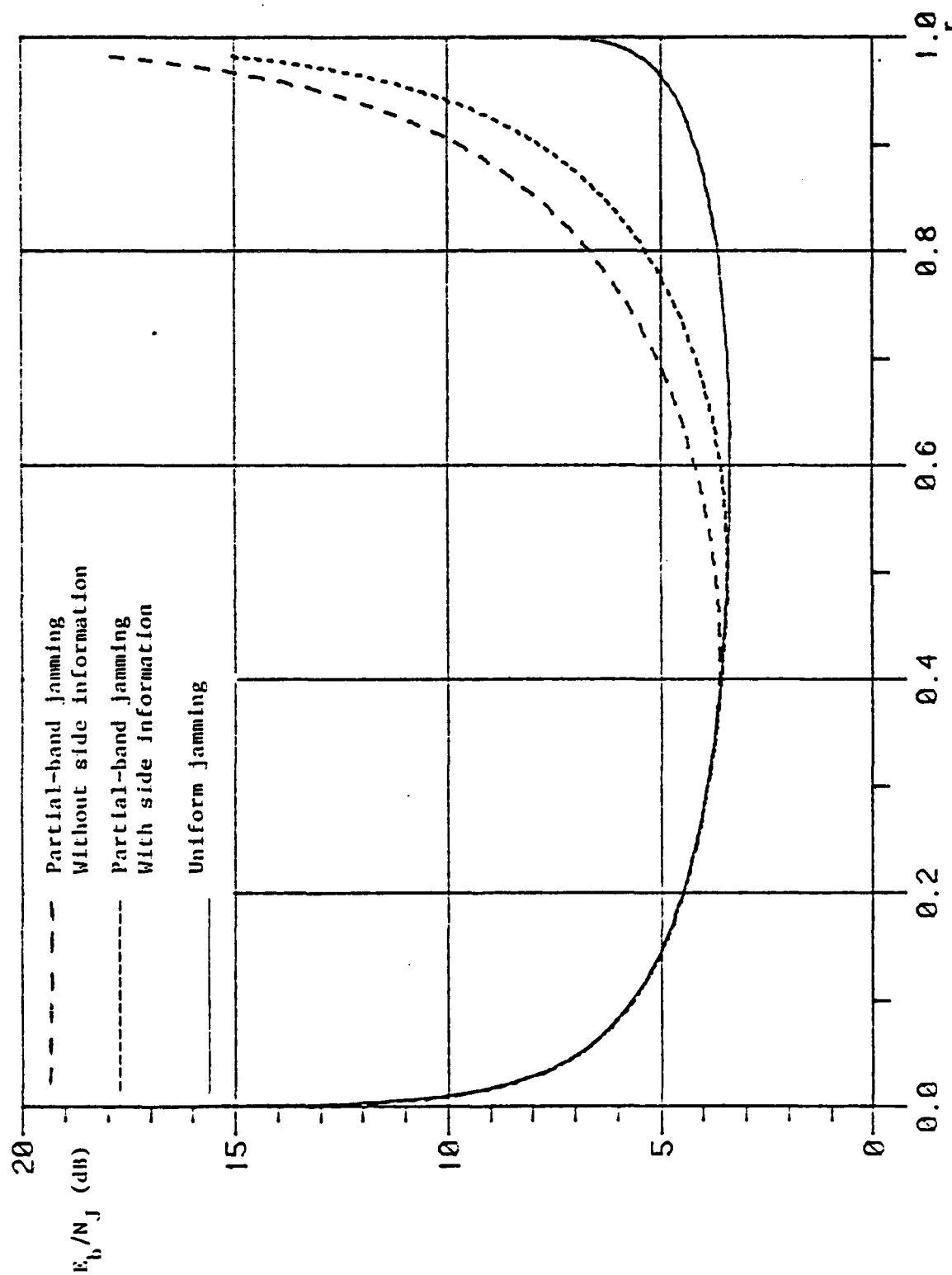


Figure 4.5. E_b/N_j needed to achieve capacity for 16-ary FSK with hard decisions and partial-band jamming.

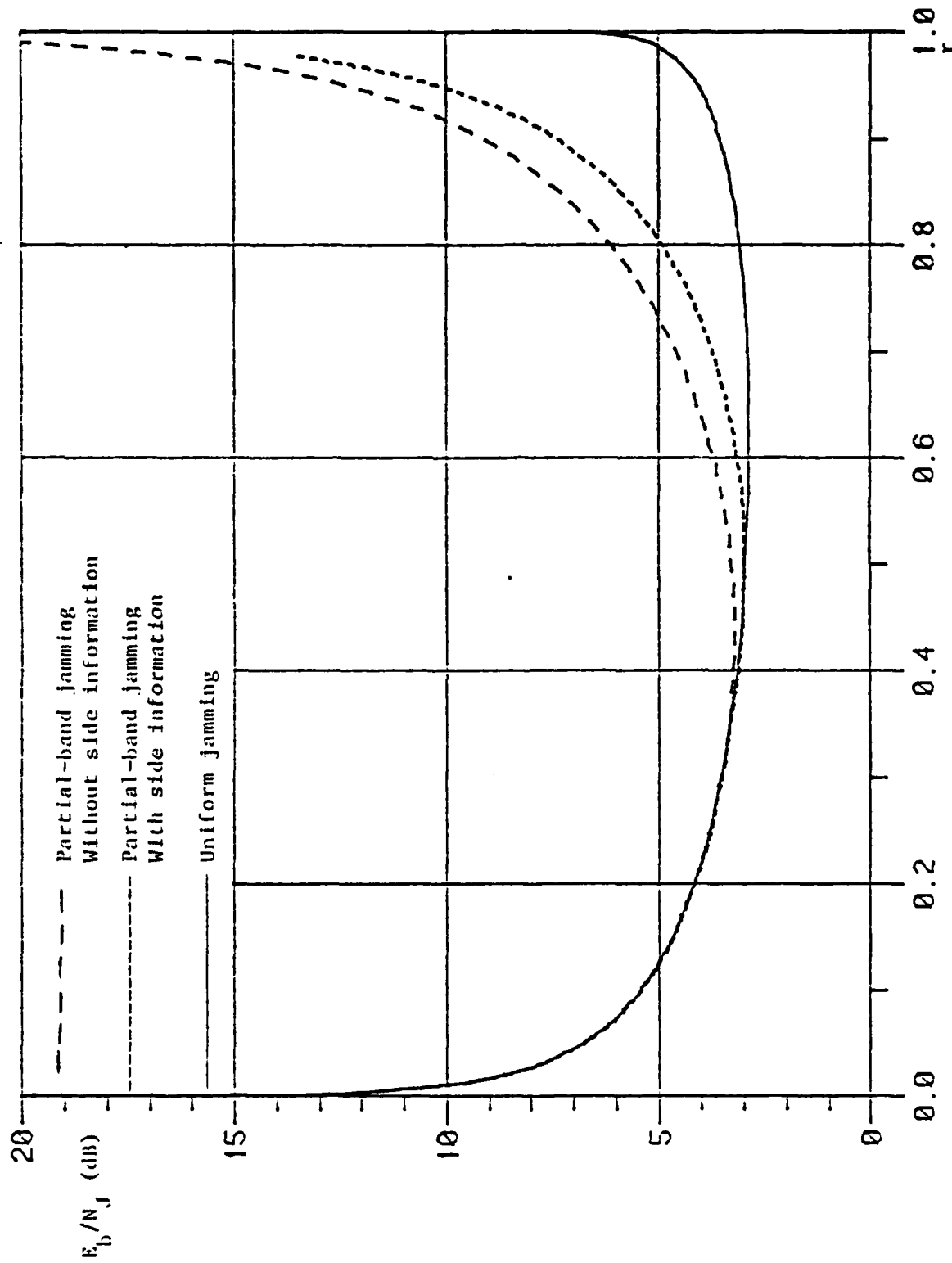


Figure 4.6. E_b/N_J needed to achieve capacity for 32-ary FSK with hard decisions and partial-band jamming.

In Section 4.5 we compare the system performance based on capacity calculation to the performance based on error probability for specific codes.

4.4 Channel Cutoff Rate

In this section we derive expressions for the computational cutoff rate for channels with partial-band jamming and noncoherent demodulation. Many of these results have appeared in the literature [4], [8], [42] for memoryless channels ($m = 1$). We repeat these calculations for completeness and also treat the case of memory $m > 1$.

Consider first the case of side information available. From (2.28) the cutoff rate with side information and memory m is given by

$$\bar{R}_0(m) = -\frac{1}{m} \log_M E\{J^m(S)\} \quad (4.23)$$

where

$$J(s) = M^{-R_{0,s}} \quad (4.24)$$

and $R_{0,s}$ is the cutoff rate of the component channels Δ_s .

The necessary assumption for the validity of (4.23) and (4.24) that the input distribution that achieves $R_{0,s}$ is the same for all component channels will be true for all channels considered.

When the jammer is on the channel it is an M -ary FSK additive Gaussian noise channel with signal energy-to-noise ratio $2E_p/N_J$. The cutoff rate $R_{0,M}(E_c/N_J)$ of this component channel is achieved with a uniform input distribution on A . When the jammer is off the channel it is a noiseless MSC with cutoff rate (measured in M -ary units) 1 achieved by a uniform input distribution. The cutoff rate of the composite channel is then

$$\bar{R}_{0,M}^{(m)}(E/N_J) = -\frac{1}{m} \log_2 \{ \bar{J}_M^{(m)}(E/N_J) \} \quad (4.25)$$

where

$$\bar{J}_M^{(m)}(E/N_J) = \max_{0 \leq \rho \leq 1} \{ \rho J_M^m(E\rho/N_J) + (1-\rho) \left(\frac{1}{M}\right)^m \} \quad (4.26)$$

and $J_M(x) = M^{-R_{0,M}(x)}$. The maximum in (4.26) can be found by setting the derivative equal to zero:

$$J_M^m(\sigma_{M,m}) + m \sigma_{M,m} J_M^{m-1}(\sigma_{M,m}) J'_M(\sigma_{M,m}) = \left(\frac{1}{M}\right)^m \quad (4.27)$$

where $\sigma_{M,m} = E\rho/N_J$ and $J'_M(x) = \partial J_M(x)/\partial x$. The value of $\sigma_{M,m}$ that satisfies (4.27) determines the worst case $\rho = \rho^*$:

$$\rho^* = \begin{cases} 1 & E/N_J < \sigma_{M,m} \\ \frac{\sigma_{M,m}}{E/N_J} & E/N_J \geq \sigma_{M,m} \end{cases} \quad (4.28)$$

Using (4.28) in (4.25) yields

$$\bar{J}_M^{(m)}(E/N_J) = \begin{cases} J_M(E/N_J) & E/N_J < \sigma_{M,m} \\ \left(\frac{1}{M}\right)^m + \frac{\Sigma_{M,m}}{E/N_J} & E/N_J \geq \sigma_{M,m} \end{cases} \quad (4.29)$$

where $\Sigma_{M,m} = \sigma_{M,m} J_M^m(\sigma_{M,m}) - M^{-m} \sigma_{M,m}$ and thus $\bar{R}_{0,M}^{(m)}$ can be found using (4.23) in (4.25). Notice from (4.28) for E/N_J the worst case jamming

strategy is uniform jamming. Using (4.29) in (4.25) we obtain

$$\bar{R}_{0,M}^{(m)}(E/N_J) = \begin{cases} R_{0,M}(E/N_J) & E/N_J < \sigma_{M,m} \\ 1 - \frac{1}{m} \log_M \frac{(1 + M^m \Sigma_{M,m})}{E/N_J} & E/N_J > \sigma_{M,m} \end{cases} \quad (4.30)$$

the constants $\Sigma_{M,m}$ and $\sigma_{M,m}$ depend on the type of receiver (e.g. hard decisions and soft decisions).

For soft decisions $J_m(x)$ can be computed to be [16]

$$J_m(x) = \frac{1 + (M-1)e^{-x} \left[\int_0^\infty t e^{-t^2/2} I_0^{\frac{1}{2}}(t\sqrt{2x}) dt \right]^2}{M} \quad (4.31)$$

For $m=1$ it is easy to check that the maximization in (4.26) is independent of M . For $m=1$ the cutoff rate with soft decisions and side information is (measured in M -ary units)

$$\bar{R}_{0,M}^{(1)}(E/N_J) = \begin{cases} R_{0,M}(E/N_J) & E/N_J < 2.871 \\ 1 - \log_M \left\{ \frac{1 + (M-1)(1.424)}{E/N_J} \right\} & E/N_J \geq 2.871 \end{cases} \quad (4.32)$$

For hard decisions $J_m(x)$ is given by [16]

$$J_m(x) = \frac{1 + (M-1) \left[\frac{M-2}{M-1} P_s(x) + 2\sqrt{P_s(x)(1-P_s(x))} / (M-1) \right]}{M} \quad (4.33)$$

where $P_s(x)$ is given in (4.18). In Table 4.2 the constants used to evaluate the cutoff rate with side information are given for $m = 1$ and $M = 2, 4, 8, 16$ and 32.

Table 4.2. Constants for M-ary hard decision cutoff rate.

M	$\sigma_{M,1}$	$\Sigma_{M,1}$
2	4.268	1.007
4	4.244	1.502
8	4.245	1.825
16	4.314	2.063
32	4.460	2.291

For hard decisions without side information and $m = 1$ the jammer just maximizes the symbol error probability. For $m > 1$ we can use (2.31) to compute the cutoff rate with $\alpha_{m,k}$ given in (4.22).

We plot in Figure 4.7 the E_b/N_J needed to achieve R_0 for binary FSK with soft decisions. Both partial-band and uniform jamming are shown. In Figure 4.8 the E_b/N_J needed is shown for binary FSK with hard decisions. Both uniform and partial-band jamming are shown as well as both cases of side information available. Finally in Figure 4.9 the corresponding results are shown for 32-ary FSK. We note here that (4.32) is similar to an expression obtained by Viterbi [43] and Omura and Levitt [31]. However, both of these papers considered soft decisions with square law combining (a suboptimum receiver). Here we consider the optimum receiver to obtain (4.32). The form of the expressions are identical with 1.424 replaced by 1.4715.

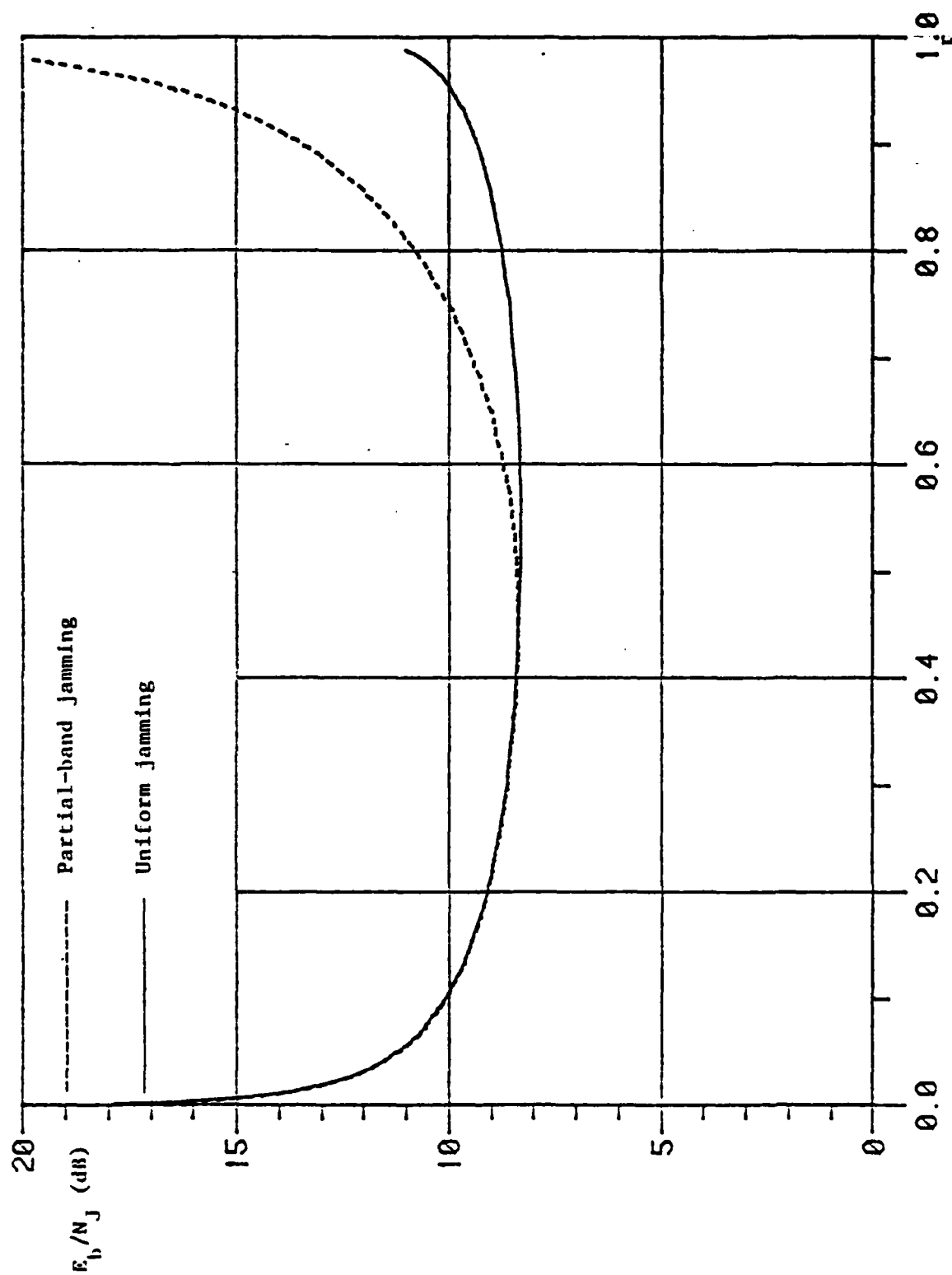


Figure 4.7. E_b/N_J needed to achieve cutoff rate binary FSK with soft decisions and partial-band jamming.

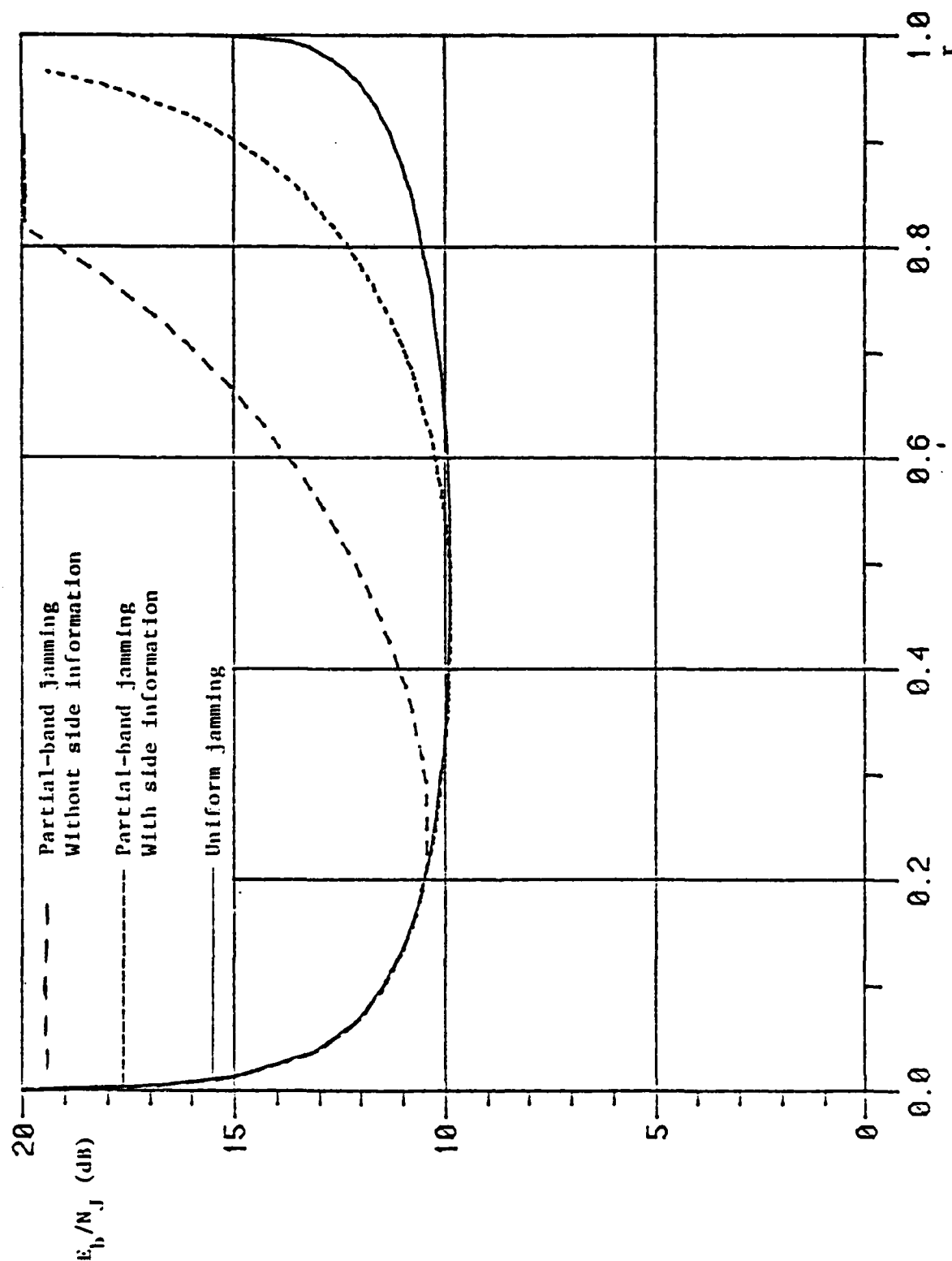


Figure 4.8. E_b/N_j needed to achieve cutoff rate for binary FSK with partial-band jamming and hard decisions.

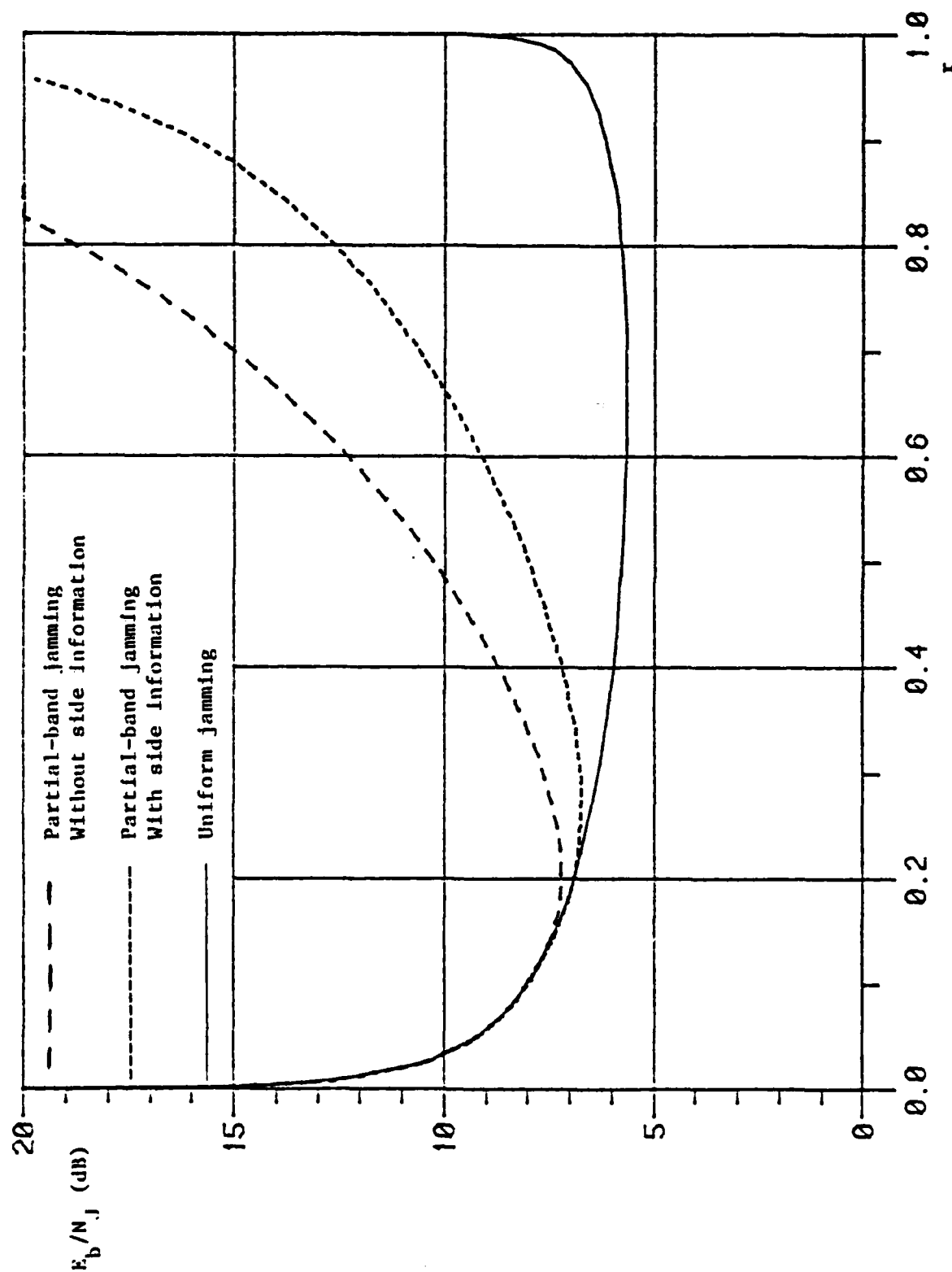


Figure 4.9. E_b/N_j needed to achieve cutoff rate for 32-ary FSK with partial-band jamming.

4.5 Performance of Codes

In this section we examine the performance of codes on channels with partial-band jamming. We consider the same codes as in Chapter 3.

Consider first hard decisions with 32-ary FSK. The symbol error probability has the exact same form for noncoherent detection as for coherent detection when the optimal duty factor ρ^* is less than one. In fact when $\rho < 1$, the decoded bit error probabilities are the same if for noncoherent we add 1.96 dB to the tables in Chapter 3. However we must check always that $\rho < 1$. In Table 4.3 we give the bit energy-to-average noise density required for 10^{-3} and 10^{-5} bit error rates with length 31 R-S codes and in Table 4.4 the corresponding curves for dual-k codes.

From capacity calculation we see that at rate $13/31=0.42$ we need $E_b/N_J=3.2$ dB for reliable communication. From cutoff rate calculations this is increased to $E_b/N_J=9.0$ dB. From Table 4.3 we see that for error probability 10^{-3} we need $E_b/N_J=7.8$ dB for R-S codes, 4.6 dB more than what the channel capacity says and 1.2 less than what the cutoff rate indicates. We note that the optimal R-S code for 10^{-3} error probability has rate 0.42 while for 10^{-5} the optimal R-S code has rate 0.35. The optimal rate from capacity considerations is 0.43 and from cutoff rate considerations is 0.191. The optimal rates for dual k codes are much less than R-S codes. For 10^{-3} error probability the rate $1/7=0.14$ is optimal while for 10^{-5} error probability the optimal rate is $1/10=0.1$ which are much less than predicted from capacity considerations and slightly less than that predicted from the cutoff rate.

Consider now the symbol error probability for repetition codes with and without side information. When side information is not available the

Table 4.3. Performance of length 31 R-S codes with bounded distance decoding, no side information and partial-band jamming (32-ary FSK).

Code	$P_{e,b} = 10^{-3}$		$P_{e,b} = 10^{-5}$	
	E_b/N_J (dB)	ρ^*	E_b/N_J (dB)	ρ^*
No Coding	22.45	0.004	42.45	0.00004
(31,29)	16.31	0.018	26.53	0.0017
(31,27)	12.99	0.039	20.33	0.008
(31,25)	11.39	0.065	16.54	0.018
(31,23)	10.12	0.095	14.64	0.034
(31,21)	9.21	0.128	13.09	0.053
(31,19)	8.58	0.164	11.98	0.075
(31,17)	8.14	0.202	11.19	0.100
(31,15)	7.91	0.242	10.66	0.127
(31,13)	7.80	0.286	10.34	0.160
(31,11)	7.89	0.331	10.23	0.193
(31,9)	8.19	0.377	10.37	0.229
(31,7)	8.78	0.424	10.79	0.267
(31,5)	9.75	0.475	11.64	0.308
(31,3)	11.50	0.528	13.30	0.350
(31,1)	15.86	0.581	17.52	0.397

Table 4.4. Performance of dual-5 codes with Viterbi decoding on channel with hard decisions, no side information available and partial-band jamming (32-ary FSK).

Coding	E_b/N_J (dB)	ρ^*	E_b/N_J (dB)	ρ^*
No Coding	23.37	0.004	45.37	0.00004
$v = 2$	14.91	0.177	22.18	0.004
3	10.89	0.325	15.18	0.064
4	9.44	0.463	12.75	0.154
5	8.93	0.584	11.40	0.262
6	8.71	0.584	10.74	0.365
7	8.67	0.688	10.70	0.461
8	8.71	0.778	10.23	0.549
9	8.80	0.857	10.16	0.628
10	8.93	0.925	10.14	0.699
11	9.07	0.986	10.17	0.764
12	9.21	1.000	10.24	0.822
13	9.34	1.000	10.32	0.875
14	9.47	1.000	10.41	0.923
15	9.56	1.000	10.51	0.966

uncoded symbol error probability is calculated using (4.20). With coding the symbol error probability is calculated using (3.55). This is plotted in Figure 4.10 for $n=1,3,5,7$. When side information is available then the symbol error probability has the form of (3.58) with different constants and P_s given in (4.18). This is plotted in Figure 4.11. With soft decisions and side information available the error probability for square-law combining has been calculated [40]. This is shown in Figure 4.12. Although square-law combining is not optimal, for low signal-to-noise ratios it is nearly optimal. With partial-band jamming the signal-to-noise ratio when jammed is typically very small so we expect that square-law combining is nearly optimal. In comparing Figures 4.12 and 3.15 we see that with noncoherent reception the optimal code rate depends on the E_b/N_J whereas for coherent reception the optimal rate is the smallest rate.

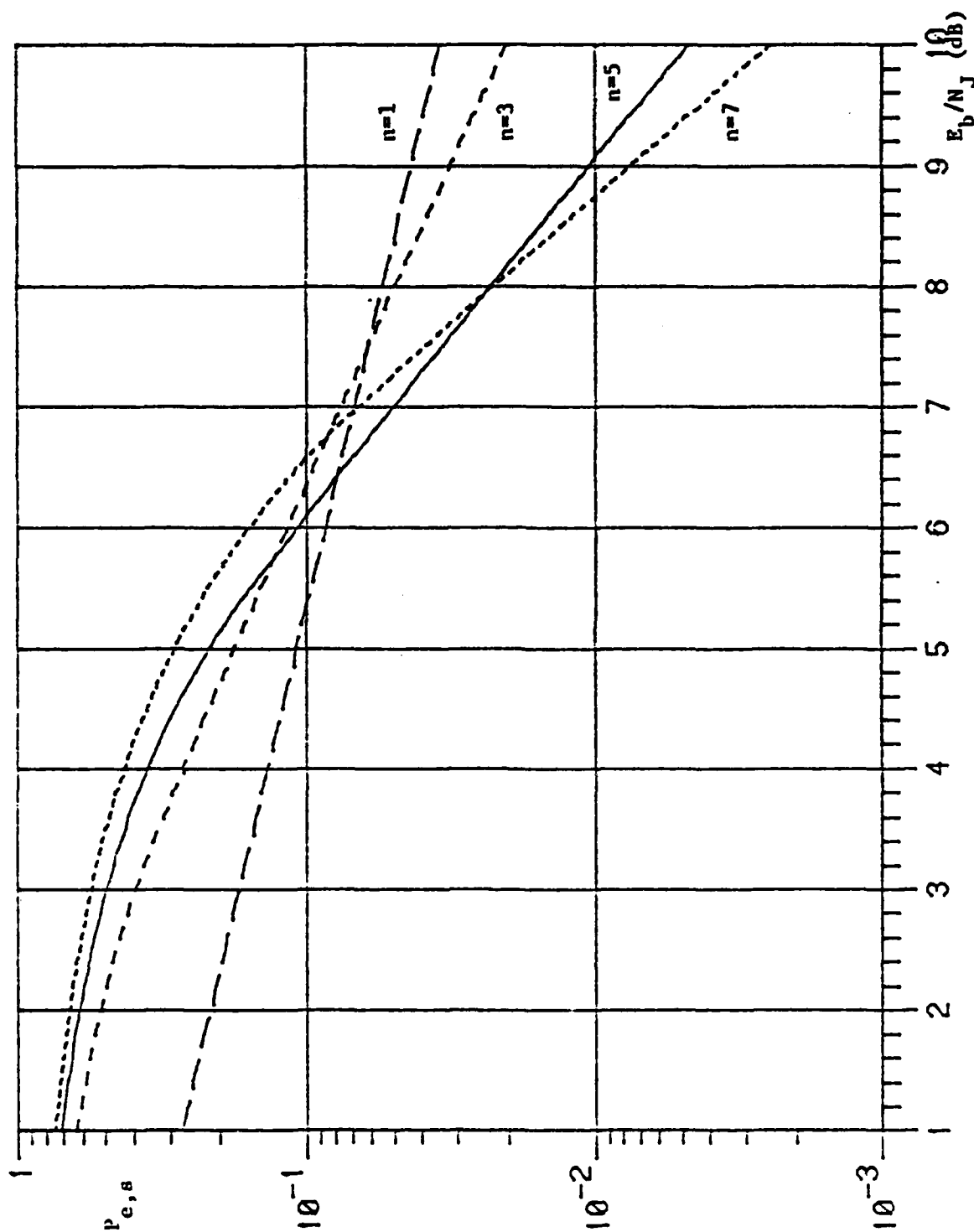


Figure 4.10. Symbol error probability for repetition codes on channel with hard decisions and no side information (32-ary FSK).

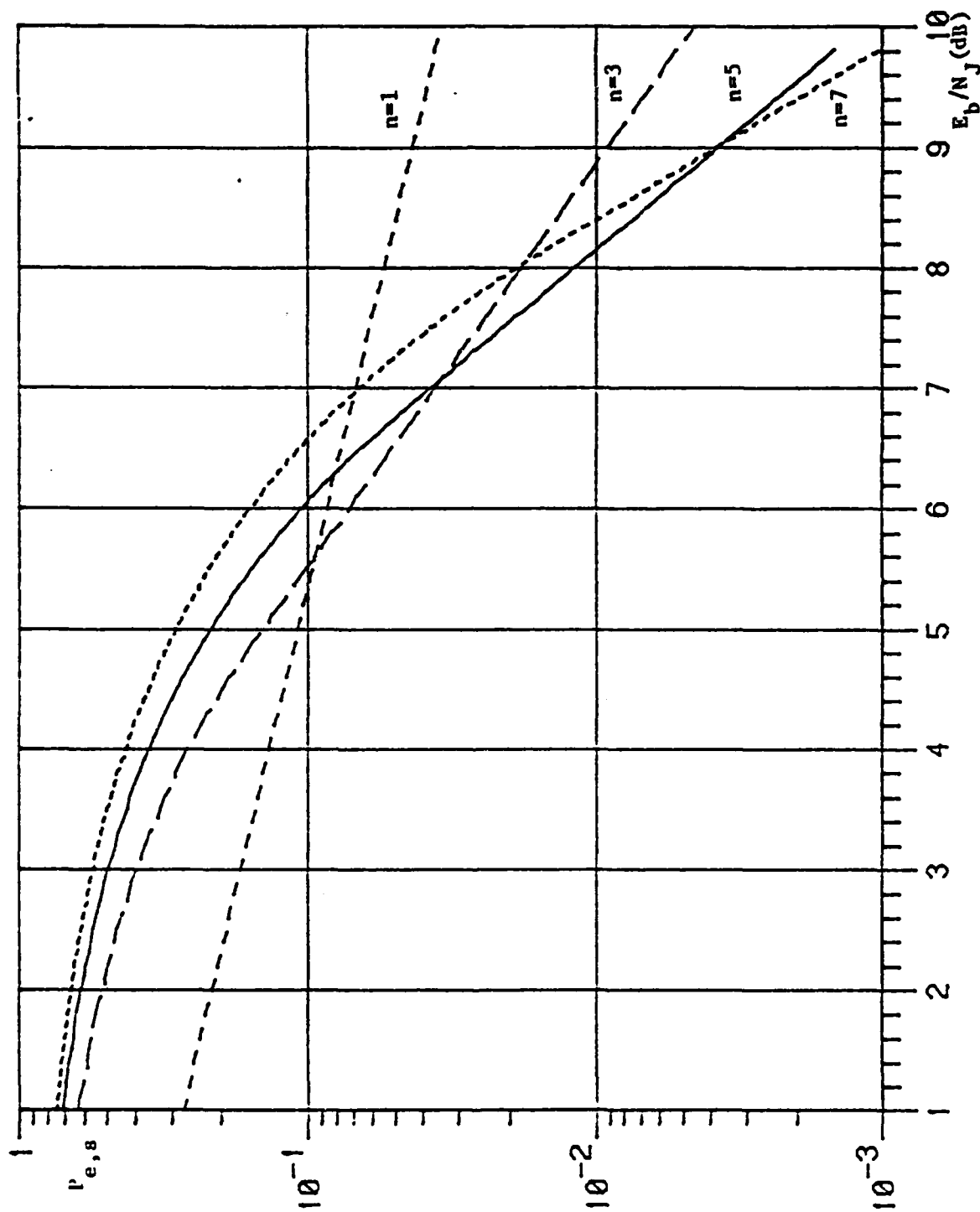


Figure 4.11. Symbol error probabilities for repetition codes on channel with hard decisions and side information available (32-ary FSK).

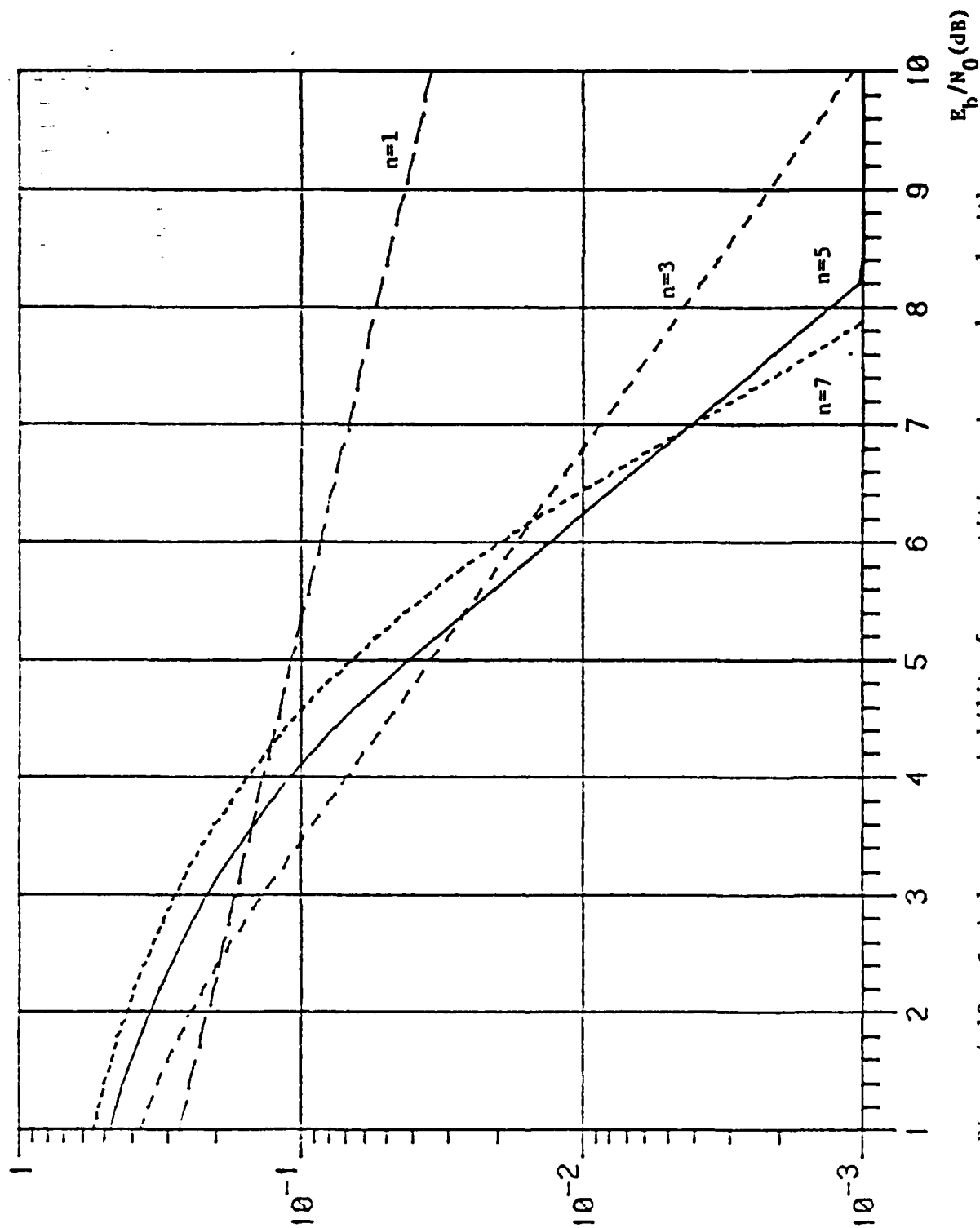


Figure 4.12. Symbol error probability for repetition codes on channel with soft decisions and side information available (32-ary FSK).

CHAPTER 5

SUMMARY AND CONCLUSIONS

In this thesis we have examined the performance of codes on channels with partial-band interference and frequency-hopping. The capacity, cutoff rate and channel capacity were all considered as performance measures. In Chapter 2 it is shown that the capacity is a better parameter to characterize the performance of a channel than the cutoff rate. Comparisons between burst-error correcting codes and random-error correcting codes with interleaving showed that the later performed comparably to the former only in the case of side information available. Without side information burst-error correcting codes perform better.

We examined extensively two types of demodulation for channels with partial-band jamming, namely coherent and noncoherent. We made the assumption that there was no background noise in the channel. The assumption is easily relaxed. The forms of nearly all expressions are modified slightly when there is some background noise. For example, the maximum symbol error probability for M-ary orthogonal signaling given in (3.29) with background noise and worst case partial-band jamming becomes

$$\bar{P}_s(E/N_J) = \begin{cases} P_s(E/(N_J+N_0)) & E/N_J < \tilde{\lambda}_M(E/N_0) \\ P_s(E/N_0) + \frac{\hat{\beta}_M(E/N_0)}{E/N_J} & E/N_J > \tilde{\lambda}_M(E/N_0) \end{cases}$$

where λ_M and β_M depend only on E/N_0 , the signal-to-background noise ratio. As $E/N_0 \rightarrow \infty$, $\tilde{\lambda}_M(E/N_0) \rightarrow \lambda_M$ given in (3.29). Similar results can be derived for the capacity and cutoff rate. These results can also be extended to include fading and jamming together. In many cases with fading

it turns out that the optimum partial-band jamming strategy is uniform or broad band jamming. For Rician fading this is true only for certain ranges of the parameter characterizing the fraction of transmitted energy that is faded. In the other range the worst case jamming strategy has the same form as in the nonfaded channel. What we try to indicate is that the channel models we are employing are quite general and applicable to a wide variety of communication systems.

For channels with partial-band interference we evaluated the performance of several codes. We considered both block and convolutional codes, hard and soft decisions and channels with and without side information. We conclude that good coding schemes exist for channels with partial-band interference and are essential for reliable communications.

APPENDIX A: DERIVATION OF CAPACITY, RANDOM CODING EXPONENT,
AND CUTOFF RATE FOR CHANNELS WITH MEMORY

In this appendix we derive (2.22), (2.24), and (2.29)-(2.32). Let Δ_s be an M-ary symmetric channel with crossover probability $s/(M-1)$ so that the symbol error probability is s . Let P be a distribution on the random variable S . Here we normalize the information rates by measuring in M-ary symbols per channel use so that the capacity is less than 1.

First consider the capacity $C_M(m)$ without side information available. From (2.16) this is given by

$$C_M(m) = \max \frac{1}{m} I(\underline{X}; \underline{Y}) \quad (A.1)$$

where $\underline{X} = (X_1, X_2, \dots, X_m)$, $\underline{Y} = (Y_1, Y_2, \dots, Y_m)$ and the maximum is over all distributions on the vector $\underline{X}$. The maximum in (A.1) is obtained by the uniform distribution for all channels Δ_s so that (A.1) can be written as

$$C_M(m) = \frac{1}{m} \sum_{\underline{Y}} \sum_{\underline{X}} p(\underline{Y}|\underline{X}) p(\underline{X}) \log_M \frac{p(\underline{Y}|\underline{X})}{p(\underline{Y})} \quad (A.2)$$

$$= \frac{M^{-m}}{m} \sum_{\underline{Y}} \sum_{\underline{X}} p(\underline{Y}|\underline{X}) \log_M \frac{p(\underline{Y}|\underline{X})}{M^{-m}} \quad (A.3)$$

That $p(\underline{Y}) = M^{-m}$ is due to the fact that the channel is symmetric and that $p(\underline{X}) = M^{-m}$. From (A.3) we have

$$\begin{aligned} C_M(m) &= \frac{M^{-m}}{m} \sum_{\underline{Y}} \sum_{\underline{X}} p(\underline{Y}|\underline{X}) (\log_M M^{-m} + \log_M p(\underline{Y}|\underline{X})) \\ &= 1 + \frac{M^{-m}}{m} \sum_{\underline{Y}} \sum_{\underline{X}} p(\underline{Y}|\underline{X}) \log_M p(\underline{Y}|\underline{X}) . \end{aligned} \quad (A.4)$$

The sum over $\underline{x}$ in (A.4) can be decomposed into two sums as

$$\sum_{\underline{x}} = \sum_{k=0}^m \sum_{\underline{x}: d(\underline{x}, \underline{y})=k} .$$

The second sum is over all vectors $\underline{x}$ which are distance k from $\underline{y}$. The distance measure here is the Hamming distance (i.e. $d(\underline{x}, \underline{y})$ is equal to the number of components in which $\underline{x}$ and $\underline{y}$ differ). If $\underline{x}$ and $\underline{y}$ differ in k places then k channel errors have occurred so that

$$\alpha_{m,k} \triangleq p(\underline{y}|\underline{x}) = E[(S/(M-1))^k (1-S)^{m-k}] ; d(\underline{x}, \underline{y}) = k . \quad (A.5)$$

Notice that (A.5) depends only on k and not on the specific $\underline{x}$ and $\underline{y}$. For $\underline{y}$ fixed, the number of vectors $\underline{x}$ such that $d(\underline{x}, \underline{y}) = k$ is just $\binom{m}{k} (M-1)^k$ so that (A.4) becomes

$$C_M(m) = 1 + \frac{1}{m} \sum_{k=0}^m \binom{m}{k} (M-1)^k \alpha_{m,k} \log_M \alpha_{m,k} \quad (A.6)$$

which for $M = 2$ is (2.22).

When side information is available the capacity $\bar{C}_M(m)$ is given by

$$\bar{C}_M(m) = E\{\hat{C}_M(S)\} \quad (A.7)$$

where $\hat{C}_M(x)$ is the capacity of an M -ary symmetric channel with symbol error probability x and is given by

$$\hat{C}_M(x) = 1 + (1-x) \log_M (1-x) + x \log_M (x/(M-1)) \quad (A.8)$$

For $M=2$ (A.7) and (A.8) yield (2.24).

Next consider the random coding exponent defined in (2.26) for these channels. For no side information available the random coding exponent is $E_o^{(M,m)}(\rho, Q^*)$ is

$$\begin{aligned}
 E_o^{(M,m)}(\rho, Q^*) &= -\frac{1}{m} \log_M \left\{ \sum_Y \left[\sum_x M^{-m} p(y|x)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right\} \\
 &= -\frac{1}{m} \log_M \left\{ \sum_Y M^{-m(1+\rho)} \left[\sum_{k=0}^m \sum_{x: d(x,y)=k} p(y|x)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right\} \\
 &= -\frac{1}{m} \log_M \left\{ \sum_Y M^{-m(1+\rho)} \left[\sum_{k=0}^m \binom{m}{k} (M-1)^k \alpha_{m,k}^{\frac{1}{1+\rho}} \right]^{1+\rho} \right\} \\
 &= \rho - \frac{1}{m} \log_M \left[\sum_{k=0}^m \binom{m}{k} (M-1)^k \alpha_{m,k}^{\frac{1}{1+\rho}} \right]^{1+\rho} \\
 &= \rho - \frac{(1+\rho)}{m} \log_M \left[\sum_{k=0}^m \binom{m}{k} (M-1)^k \alpha_{m,k}^{\frac{1}{1+\rho}} \right] \quad (A.9)
 \end{aligned}$$

which for $M=2$ is (2.29).

For the case of side information available $\bar{E}_o^{(M,m)}(\rho, Q^*)$ can be calculated as follows

$$\begin{aligned}
 \bar{E}_o^{(M,m)}(\rho, Q^*) &= -\frac{1}{m} \log_M \left(\sum_{Y,s} \left[\sum_x M^{-m} p(y,s|x)^{\frac{1}{1+\rho}} \right]^{1+\rho} \right) \\
 &= -\frac{1}{m} \log_M \left(\sum_{Y,s} M^{-m(1+\rho)} \left[\sum_{k=0}^m \sum_{x: d(x,y)=k} (p(y|x)p(s))^{1/(1+\rho)} \right]^{1+\rho} \right) \\
 &= -\frac{1}{m} \log_M \left(\sum_{Y,s} M^{-m(1+\rho)} \left[\sum_{k=0}^m \binom{m}{k} (M-1)^k \left\{ (s/(M-1))^k (1-s)^{m-k} p(s) \right\}^{1/(1+\rho)} \right]^{1+\rho} \right) \\
 &= \rho - \frac{1}{m} \log_M E \left\{ \sum_{k=0}^m \binom{m}{k} (M-1)^k \left[\left(\frac{s}{M-1} \right)^k (1-s)^{m-k} \right]^{1/(1+\rho)} \right\}^{1+\rho} \quad (A.10)
 \end{aligned}$$

which for $M=2$ is (2.30).

The cutoff rate can be easily evaluated by setting $\rho = 1.0$ in (A.9) and (A.10). When side information is not available (A.9) with $\rho = 1.0$ becomes

$$R_{0,M}(m) = 1 - \frac{2}{m} \log_M \sum_{k=0}^M \binom{m}{k} (M-1)^k (\alpha_{m,k})^{\frac{1}{2}} \quad (\text{A.11})$$

which for $M=2$ is (2.31). When side information is available (A.10) with $\rho = 1.0$ becomes

$$\begin{aligned} \bar{R}_{0,M}(m) &= 1 - \frac{1}{m} \log_M^E \left\{ \sum_{k=0}^m \binom{m}{k} (M-1)^k \left[\left(\frac{S}{M-1} \right)^k (1-S)^{m-k} \right]^{\frac{1}{2}} \right\}^2 \\ &= 1 - \frac{1}{m} \log_M^E \sum_{k=0}^m \sum_{\ell=0}^m \binom{m}{k} \binom{m}{\ell} (M-1)^{k+\ell} \left[\left(\frac{S}{M-1} \right)^{k+\ell} (1-S)^{2m-k-\ell} \right]^{\frac{1}{2}} \\ &= 1 - \frac{1}{m} \log_M \left(\sum_{k=0}^m \sum_{\ell=0}^m \binom{m}{k} \binom{m}{\ell} (M-1)^{k+\ell} \alpha_{m, \frac{k+\ell}{2}} \right) \end{aligned} \quad (\text{A.12})$$

which for $M=2$ is (2.32).

APPENDIX B

WORST CASE DISTRIBUTION FOR PARTIAL-BAND JAMMING

In this appendix we show that allowing the jammer to have an arbitrary number of power levels instead of just on or off does not change the optimal jamming strategy. Viterbi and Jacobs showed based on an upper bound to the error probability that for binary FSK two level is optimum with diversity. Here we prove that two levels is optimum for binary FSK based on the exact bit error probability and that two levels is optimal based on channel capacity when side information is available.

Let Z be a nonnegative random variable with expectation N and distribution $F_Z(z)$. If $Z = z$ represents the jammer having noise level z then the average error probability $\bar{p}$ is δ

$$\bar{p} = E\left\{\frac{1}{2} e^{-\delta/2Z}\right\} \quad (B.1)$$

where δ is the received energy of the transmitted signal. Define the function $f(z)$ by

$$f(z) = \begin{cases} \frac{1}{2} e^{-\delta/2z} & z > 0 \\ 0 & z = 0 \end{cases}$$

This is shown in Figure B.1.

We will show that f has a single point of inflection

$$f'(z) = \frac{1}{2} e^{-\delta/2z} (\delta/2z^2)$$

$$f''(z) = \frac{1}{2} e^{-\delta/2z} (\delta/z^3) \left[\frac{E}{4z} - 1 \right]$$

Since $\frac{1}{2} e^{-\delta/2z} (\frac{\delta}{z})$ is always nonnegative the only point of inflection occurs at $z = E/4$. Furthermore for $z < E/4$, $f(z)$ is a convex function while for $z > E/4$ $f(z)$ is a concave function. Define the function $\tilde{f}$ by

$$\tilde{f}(z) = \begin{cases} e^{-1} z/E & 0 \leq z \leq E/2 \\ f(z) & z > E/2 \end{cases}$$

This function is shown in Figure A.1. From the above it can be shown that

$$f(z) \leq \tilde{f}(z) \quad z \geq 0$$

with equality if $z > E/2$. We can write (A.1) as

$$\bar{p} = E\{f(Z)\} \leq E\{\tilde{f}(Z)\} \quad (\text{B.2})$$

with equality if $z > E/2$ or if Z is concentrated at the two endpoints i.e. $z = 0$ and $z = E/2$. Now since $\tilde{f}$ is a concave function we have

$$\bar{p} \leq E(\tilde{f}(Z)) \leq \tilde{f}(E(Z)) = \tilde{f}(N) \quad (\text{B.3})$$

Equality can be achieved in (B.3) if z is concentrated on two points or less. Notice that

$$\tilde{f}(N) = \begin{cases} \frac{1}{2} e^{-\delta/2N} & \delta/N < 2 \\ \frac{e^{-1}}{\delta/N} & \delta/N \geq 2 \end{cases}$$

Thus we have shown that two levels is a worst-case distribution for binary FSK with error probability on the performance measure. The capacity without side information is a decreasing function of the error probability so that two levels is optimum without side information also.

With side information the capacity $\bar{C}$ is the average of the capacities of various power levels:

$$\bar{C} = E\{C(\mathcal{G}/Z)\} \quad .$$

Now instead of maximizing the error probability we minimize the capacity. All the arguments for error probability are true when f is replaced by $C(\mathcal{G}/z)$ provided $C(\mathcal{G}/z) = g(z)$ changes convexity just once. This is much harder to show for g than for f and will not be done here.

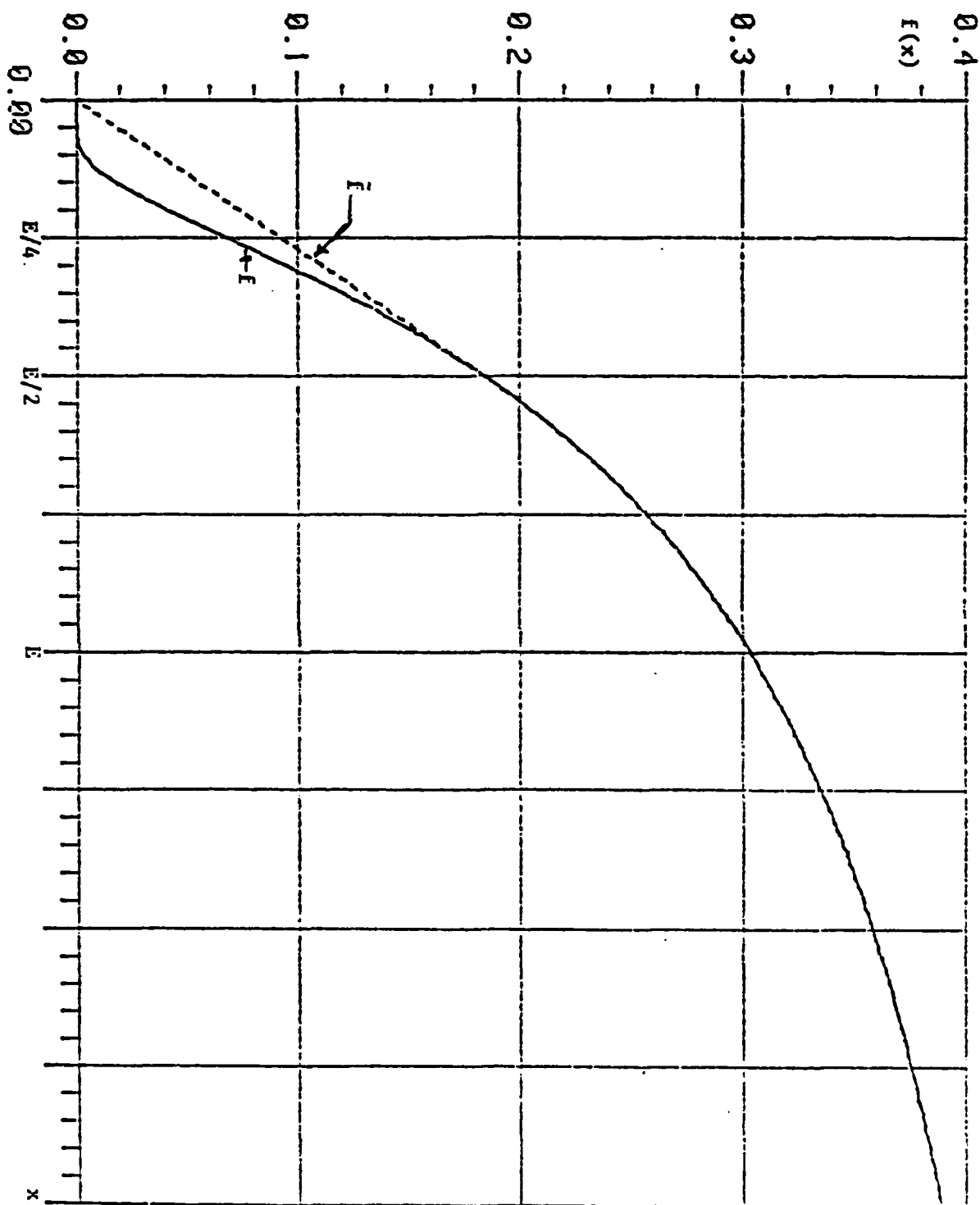


Figure A.1. The functions f and $\bar{f}$.

APPENDIX C: ERROR PROBABILITY FOR REPETITION CODES
ON M-ARY SYMMETRIC CHANNELS

In this appendix we derive the error probability for repetition codes on an M-ary symmetric channel (MSC). Let p be the probability of a symbol error on an MSC and let $q=1-p$. Also let X represent the input to the channel ($X \in \{0,1,\dots,M-1\}$) and Y the output. Then the probability that $Y=y$ given that $X=x$ is given by

$$P\{Y=y|X=x\} = \begin{cases} q, & x=y \\ p/M-1 & x \neq y \end{cases}$$

Assume the information symbol to be transmitted is $X=0$. The repetition code sends this symbol n times. The decoder counts the number of times each symbol was received and chooses the one that had the largest count, as the transmitted symbol. Let Y_i $0 \leq i \leq M-1$ be the number of times that i was received. For $n=1$ the symbol error probability $P_{e,s}(1)$ is just p ; for $n=2$ the error probability $P_{e,s}(2)$ can be computed by considering the probability of correct decision $P_{c,s}$:

$$P_{c,s}(n) = 1 - P_{e,s}(n) \quad (C.1)$$

This can be computed as

$$P_{c,s}^{(n)} = P\{Y_0=n\} + \frac{1}{2}P\{Y_0=1, Y_j=1, \text{ some } j \neq 0\}$$

The first term is the probability that both symbols transmitted were received correctly and is equal to $(1-p)^2$. The second term is the probability that a tie occurred which is decided randomly between $X=0$ and $X=j$. This is given by $\frac{1}{2} 2(1-p)p$ so that

$$P_{c,2} = (1-p)^2 + p(1-p) = 1-p \quad (C.2)$$

For $n=3$ we have the probability of correctly decoding $P_{c,s}(3)$ given by

$$\begin{aligned} P_{c,s} &= P\{Y_0 \geq 2\} + \frac{1}{3}P\{Y_0=1, Y_1=1, Y_j=1, i \neq 0, j \neq 0, i \neq 1\} \\ &= q^3 + 3pq^2 + \frac{1}{3} 3qp \left(\frac{M-2}{M-1} p\right) \\ &= q^3 + 3pq^2 + \left(\frac{M-2}{M-1}\right)p^2 q \quad (C.3) \end{aligned}$$

For $n=4$ we have

$$\begin{aligned} P_{c,s}(4) &= q^4 + 4q^3 p + 6q^2 p \left(\frac{M-2}{M-1} p\right) + \frac{1}{2} 6q^2 p \frac{p}{M-1} \\ &\quad + \frac{1}{4} 4qp \left(\frac{M-2}{M-1} p\right) \left(\frac{M-3}{M-1} p\right) \\ &= q^4 + 4q^3 p + \left[6\left(\frac{M-2}{M-1}\right) + 3\left(\frac{1}{M-1}\right)\right] q^2 p^2 + \frac{(M-2)(M-3)}{(M-1)^2} qp^3 \\ &\quad (C.4) \end{aligned}$$

For $n=5$

$$\begin{aligned} P_{c,s}(5) &= q^5 + 5q^4 p + 10q^3 p^2 + \left[10\left(\frac{M-2}{M-1}\right)\left(\frac{M-3}{M-1}\right) + 15 \frac{M-2}{(M-1)^2}\right] q^2 p^3 \\ &\quad + \frac{(M-2)(M-3)(M-4)}{(M-1)^3} qp^4 \quad (C.5) \end{aligned}$$

For $n=6$

$$\begin{aligned}
P_{c,s}(6) = & q^6 + 6q^5p + 15q^4p^2 + \left[60 \frac{(M-2)}{(M-1)^2} + 20 \frac{(M-2)(M-3)}{(M-1)^2} + \frac{10}{(M-1)^2} \right] q^3p^3 \\
& + \left[15 \frac{(M-2)(M-3)(M-4)}{(M-1)^3} + 15 \frac{M-2}{(M-1)^3} \right] q^2p^4 \\
& + \left[\frac{(M-2)(M-3)(M-4)(M-5)}{(M-1)^4} \right] qp^5. \tag{C.6}
\end{aligned}$$

Notice in each case that $P_{c,s}(n)$ is expressed as

$$P_{c,s}(n) = \sum_{i=0}^{n-1} a_i q^{n-i} p^i \tag{C.7}$$

For $n=7$ the coefficients are

i	a_i
0	1
1	7
2	21
3	35
4	$35 \left[6 \frac{(M-2)(M-3)}{(M-1)^3} + \frac{(M-2)(M-3)(M-4)}{(M-1)^3} + 2 \frac{M-2}{(M-1)^4} \right]$
5	$21 \left[\frac{(M-2)(M-3)(M-4)(M-5)}{(M-1)^4} + 5 \frac{(M-2)(M-3)(M-4)}{(M-1)^4} \right.$
	$\left. + 5 \frac{(M-2)(M-3)}{(M-1)^4} \right]$
6	$\frac{(M-2)(M-3)(M-4)(M-5)}{(M-1)^5}$

For $n=8$ and $M=32$ the a_i are given below.

i	a_i
1	1.
2	8.
3	28.
4	56.
5	69.998825149
6	55.717975016
7	21.909972461
8	0.481708426

For any M and n with $p = \frac{M-1}{M}$, $P_{e,c}(n) = (M-1)/M$.

We can calculate an upper bound on $P_{e,c}(n)$ for any n by applying the union bound technique. This is calculated as follows:

$$P_{e,s}(n) \leq (M-1) P_{e,s}^{(2)}(n)$$

where $P_{e,s}^{(2)}(n)$ is the error probability between two codewords of a repetition code of length n . This can be shown to be given by

$$\begin{aligned}
 P_{e,s}^{(2)}(n) = & \sum_{\substack{j,k \\ j < k \\ j+k \leq n}} \binom{n}{j} q^j \binom{n-j}{k} \left(\frac{p}{M-1}\right)^k \left(\frac{M-2}{M-1} p\right)^{n-j-k} \\
 & + \frac{1}{2} \sum_{j=0}^{\lfloor n/2 \rfloor} \binom{n}{j} q^j \binom{n-j}{j} \left(\frac{p}{M-1}\right)^j \left(\frac{M-2}{M-1} p\right)^{n-2j}
 \end{aligned} \tag{C.8}$$

A simpler bound can be obtained by using the Bhattacharyya bound on $P_{e,s}^{(2)}(n)$. This bound is

$$P_{e,s}^{(2)}(n) \leq D^n \tag{C.9}$$

where D is given as

$$D = \left(\frac{M-2}{M-1} \right) p + 2\sqrt{p(1-p)/M-1} .$$

REFERENCES

1. E.R. Berlekamp, "The technology of error-correcting codes," Proc. IEEE vol. 68, May 1980.
2. S.L. Bernstein et al., "Variable rate Viterbi decoding in the presence of RFI," National Telecommunications Conference Record, pp. 36.6.1-36.6.5, Dec 1977.
3. N.M. Blachman, "Communication as a game," Wescon 1957 Conference Record, 1957.
4. E.A. Bucher, "Coding options for efficient communication on non-stationary channels," National Telecommunications Conference Record, pp. 4.1.1-4.1.7, Dec. 1980.
5. S.A. Butman, et. al., "Design criteria for noncoherent Gaussian channels with MFSK signaling and coding," IEEE Trans. Commun., vol. COM-24, pp. 1078-1088, October 1976.
6. S.A. Butman and R.J. McEliece, "The ultimate limits of binary coding for a wideband Gaussian channel," JPL Deep Space Network Progress Report, no. 42-22 (1974), pp. 78-80.
7. J.B. Cain and J.M. Geist, "Interleaving considerations for coding on Gaussian noise channels with burst erasures," National Telecommunications Conference Record, pp. 44.5.1-44.5.5, Nov. 1979.
8. J.B. Cain and J.M. Geist, "Modulation, coding and interleaving tradeoffs for spread spectrum systems," National Telecommunications Conference Record, pp. B7.3.1-B7.3.5, Nov. 1981.
9. G.C. Clark and J.B. Cain, Error-Correction Coding for Digital Communications, New York: Plenum Press, 1981.
10. I. Csiszar and J. Korner, Information Theory: Coding Theorems for Discrete Memoryless Systems, New York: Academic Press, 1981.
11. R.C. Dixon, Spread Spectrum Techniques. New York: IEEE Press, 1976.
12. R.L. Dobrushin, "Optimum information transmission through a channel with unknown parameters," Radio Engineering Electronics, vol. 4 no. 12, 1959.

13. R.G. Gallager, Information Theory and Reliable Communication. New York: Wiley, 1968.
14. E.A. Geraniotis and M.B. Pursley, "Error probabilities for slow-frequency-hopped spread-spectrum multiple access communications over fading channels," IEEE Trans. Commun., vol. COM-31, May 1982.
15. S.W. Houston, "Modulation techniques for communication, Part 1: Tone and noise jamming performance of spread spectrum M-ary FSK and 2,4-ary DPSK waveforms," Proc. IEEE National Aerospace and Electronics Conference, pp. 51-58, June 1975.
16. K.L. Jordan, "The performance of sequential decoding in conjunction with efficient modulation," IEEE Trans. Commun. Tech., vol. COM-14, pp. 283-297, June 1965.
17. H. Kesten, "Some remarks on the capacity of compound channels in the semicontinuous case," Information and Control vol. 4, pp. 169-184, 1961.
18. B.K. Levitt, "Effect of modulation format and jamming spectrum on performance of direct sequence spread spectrum systems," National Telecommunications Conference Record, pp. 3.4.1-3.4.5, Dec. 1980.
19. B.K. Levitt, J.K. Omura, "Coding tradeoffs for improved performance of FH/MFSK systems in partial band noise," National Telecommunications Conference Record, pp. D9.1.1-D9.1.5, Dec. 1981.
20. W.C. Lindsey and M.K. Simon, Telecommunication Systems Engineering. New Jersey: Prentice-Hall, 1973.
21. D.R. Martin and P.L. McAdam, "Convolutional code performance with optimal jamming," IEEE International Conference on Communications, Conference Record, pp. 4.3.1-4.3.7, June 1980.
22. J.L. Massey, "Capacity, cutoff rate, and coding for a direct-detection optical channel," IEEE Trans. Commun., vol. COM-29, pp. 1615-1621, Nov. 1981.
23. J.L. Massey, "Coding and modulation in digital communications," in Proc. Int. Zurich Sem. on Digital Communications, Zurich, Switzerland, Mar. 1974.

24. R.J. McEliece, "Practical codes for photon communication," IEEE Trans. Inform. Theory, vol. IT-27, pp. 393-398, July 1981.
25. R.J. McEliece, "RFI channels," Jet Propulsion Laboratory Deep Space Network Progress Report, 42-60, pp. 103-106, 1980.
26. R.J. McEliece, "RFI channels, II," Jet Propulsion Laboratory Deep Space Network Progress Report, in press.
27. R.J. McEliece, The Theory of Information and Coding. Reading, Ma: Addison-Wesley, 1977.
28. R.J. McEliece and W.E. Stark, "An information theoretic study of communication in the presence of jamming," IEEE International Conference on Communication. Conference Record, pp. 45.3.1-45.3.5, June 1981.
29. R.J. McEliece and W.E. Stark, "Channels with block interference," submitted to IEEE Trans. Information Theory, Nov. 1981..
30. J.P. Odenwalder, "Dual-K convolutional codes for noncoherent demodulated channels," IEEE International Telecommunications Conf., pp. 165-176, 1976.
31. J.K. Omura and B.K. Levitt, "A general analysis of anti-jam communication systems," National Telecommunications Conference Record, pp. B7.1.1-B7.1.5, Dec. 1981.
32. M.B. Pursley, "Coding and diversity for channels with fading and pulsed interference," Proc. 1982 Conf. Information Sciences and Systems, Princeton N.J., Mar. 1982.
33. W.L. Root, "Communication through unspecified additive noise," Information and Control, vol. 4, pp. 15-29, 1961.
34. C.E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J., vol. 27, pp. 623-656, Oct. 1948.
35. M.K. Simon and A. Polydoros, "Coherent detection of frequency-hopped quadrature modulation in the presence of jamming - Part I: QPSK and QASK modulations. IEEE Trans. Commun. vol. COM-29, pp. 1644-1660, Nov. 1981.

36. W.E. Stark, "Performance of concatenated codes of channels with jamming," IEEE International Conference on Communications, Conference Record, June 1982.
37. W.E. Stark and R.J. McEliece, "Capacity and Coding in the presence of fading and jamming," National Telecommunications Conference Record, pp. B7.4.1-B7.4.5, Nov. 1981.
38. J. Stoer and C. Witzgall, Convexity and Optimization in Finite Dimensions I. New York: Springer-Verlag, 1970.
39. D.J. Torrieri, Principles of Military Communication Systems. Dedham, Mass.: Artech, 1981.
40. B.D. Trumpis, "On the optimum detection of fast frequency hopped MFSK signals in worst case jamming," preprint.
41. B.D. Trumpis and P.L. McAdam, "Performance of convolutional codes on burst noise channels," National Telecommunications Conference Record, pp. 36:3-1-36:3-14, Dec. 1977.
42. A.J. Viterbi, "No parameter for a pulse-burst channel," presented at the 1979 International Symposium on Information Theory, June 1979.
43. A.J. Viterbi, "Spread-spectrum communications-myths and realities," IEEE Commun. Mag., vol. 4, pp. 11-18, May 1979.
44. A.J. Viterbi and I.M. Jacobs, "Advances in coding and modulation for noncoherent channels affected by fading, partial band, and multiple-access interference," in Advances in Communication Systems, vol. 4. New York: Academic, 1975.
45. A.J. Viterbi and J.K. Omura, Principles of Digital Communication and Coding. New York: Academic, 1975.
46. J. Wolfowitz, Coding Theorems of Information Theory, 3rd Ed. Berlin: Springer-Verlag, 1978.
47. J.M. Wozencraft and I.M. Jacobs, Principles of Communication Engineering. New York: Wiley, 1965.

VITA

Wayne Eric Stark was born in Harvey, Illinois on February 26, 1956. He received the B.S degree with highest honors from the University of Illinois in 1978 and the M.S degree from the University of Illinois in 1979. From August 1978 till June 1982 he was a Research Assistant in the Coordinated Science Laboratory. He has co-authored the following papers:

"Bounds on error probability for direct-sequence spread-spectrum multiple-access communications," MIDCON Conference Proceedings, paper 15/1, pp. 1-14, November 1979. (with D.E. Borth, M.B. Pursley and D.V. Sarwate)

"On the average probability of error for direct-sequence spread-spectrum multiple-access systems," Proc. of the 1980 Conference on Information Sciences and Systems, pp.320-325, Princeton University, Princeton, NJ, March 1980. (with M.B. Pursley and D.V. Sarwate)

"Kronecker sequences for spread-spectrum communication," Proc. of the 1980 Conference of Information Sciences and Systems, pp. 326-329, Princeton University, Princeton, NJ, March 1980. (with D.V. Sarwate)

"Kronecker sequences for spread-spectrum communication," IEE Proc., Part F: Communications, Radar, and Signal Processing, vol. 128, pp. 104-107 April 1981. (with D.V. Sarwate)

"An information theoretic study of communication in the presence of jamming," IEEE International Conference on Communications, Conference Record, pp. 45.3.1-45.3.5, June, 1981. (with R.J. McEliece)

"Error probability for direct-sequence spread-spectrum communications-Part I: Upper and lower bounds," IEEE Trans. Commun., COM-30, pp.975-984 (with M.B. Pursley and D.V. Sarwate)

"Capacity and coding in the presence of fading and jamming," IEEE National Telecommunications Conference Record, pp. B7.4.1-B7.4.5, Nov. 1981. (with R.J. McEliece)

"Performance of concatenated codes on channels with jamming," to appear in the International Conference on Communications, Conference Record, June 1982.