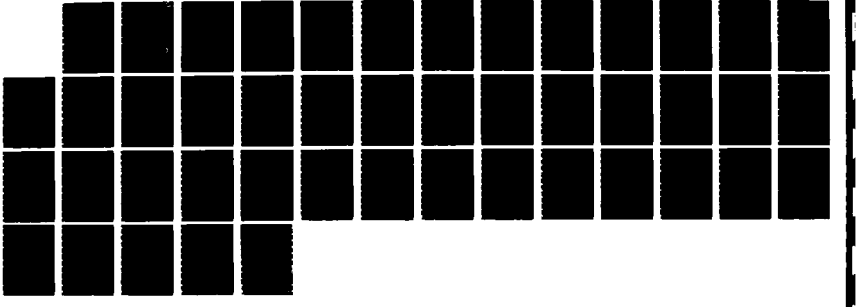
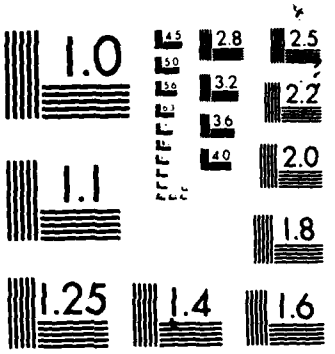
AD-A172 875 GAUSSIAN ARBITRARILY VARYING CHANNELS(U) MARYLAND UNIV 1/1
COLLEGE PARK DEPT OF ELECTRICAL ENGINEERING
B HUGHES ET AL. 30 SEP 86 NRL-8971 N00014-83-G-0192
UNCLASSIFIED F/G 17/2 NL





Naval Research Laboratory
Washington, DC 20375-5000 NRL Report 8971 September 30, 1986

Gaussian Arbitrarily Varying Channels

BRIAN HUGHES AND PRAKASH NARAYAN

Electrical Engineering Department
University of Maryland
College Park, Maryland 20742

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution unlimited.
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) NRL Report 8971	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION University of Maryland 6b OFFICE SYMBOL (If applicable)	7a NAME OF MONITORING ORGANIZATION Naval Research Laboratory
6c ADDRESS (City, State, and ZIP Code) College Park, MD 20742	7b ADDRESS (City, State, and ZIP Code) Washington, DC 20375-5000
8a NAME OF FUNDING / SPONSORING ORGANIZATION Office of Naval Research 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER Grant No: N00014-83-G-0192 Grant No: N00014-84-G-0101
8c ADDRESS (City, State, and ZIP Code) Arlington, VA 22217	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO: 61153N PROJECT NO: TASK NO: RR02105-42 WORK UNIT ACCESSION NO: DN880-011

11 TITLE (Include Security Classification)
Gaussian Arbitrarily Varying Channels

12 PERSONAL AUTHOR(S)
Hughes, Brian and Narayan, Prakash

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Interim	FROM 9/1/83 TO 8/26/85	1986 September 30	44

16 SUPPLEMENTARY NOTATION
(See page ii)

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Arbitrarily varying channels; Capacity; Jammed communications; Gaussian channels

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The Arbitrarily Varying Channel (AVC) can be interpreted as a model of a channel jammed by an intelligent and unpredictable adversary. In this report, we investigate the asymptotic reliability of optimum random block codes on *Gaussian* Arbitrarily Varying Channels (GAVCs). A GAVC is a discrete-time, memoryless Gaussian channel with input power P_T and noise power N_e, which is further corrupted by an additive "jamming signal." The statistics of this signal are unknown and may be arbitrary, except that they are subject to a power constraint P_J.

We distinguish between two types of power constraints: *peak* and *average*. For peak constraints on the input power and the jamming power, we show that the GAVC has a (strong) capacity. For the remaining cases, in which the transmitter and/or the jammer are subject to average power constraints, only capacities are found. The asymptotic error probabilities suffered by optimal random codes in these cases are determined. Our results suggest that if the jammer is subject only to an average power constraint, reliable communication is impossible at any positive code rate.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL Dennis N. McGregor	22b TELEPHONE (Include Area Code) (202) 767-2952 22c OFFICE SYMBOL Code 7521

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

16. SUPPLEMENTARY NOTATION

This research was sponsored by the Naval Research Laboratory and the Office of Naval Research under grants Nos. N00014-83-G-0192 and N00014-84-G-0101, the National Science Foundation under grant No. ECS-82-0444-9, and the Minta Martin Fund for Aerospace Research from the University of Maryland. The material in this report was presented in part at the 19th Annual Conference on Information Sciences and Systems, The Johns Hopkins University, March 27-29, 1985. B. Hughes was with the Electrical Engineering Department of the University of Maryland, College Park, MD 20742. He is now with the Department of Electrical Engineering and Computer Science of the Johns Hopkins University, Baltimore, MD 21218. P. Narayan is with the Electrical Engineering Department of the University of Maryland, College Park, MD 20742.

CONTENTS

GAUSSIAN ARBITRARILY VARYING CHANNELS

1. INTRODUCTION

Consider the following communications channel (cf. Fig. 1). Once each second, the transmitter chooses for transmission to the receiver an arbitrary real number, say u_i at time i, such that the sequence $\{ u_i \}$ satisfies a power constraint P_T (to be made precise below). In transmission, this number is corrupted in such a way that it is received as $u_i + n_{ei}^* + s_i$. The elements of the sequence $\{ n_{ei}^* \}$ are independent, zero-mean Gaussian random variables, each having variance N_e. The transmitter and the receiver have no knowledge of the sequence $\{ s_i \}$, other than that it satisfies a certain power constraint, say P_J (also to be made precise below). The sequence $\{ s_i \}$ may have arbitrary, time-varying, possibly non-Gaussian statistics. The goal of the transmitter and receiver is to construct a coding system to reliably convey discrete source data over this channel, knowing only N_e, P_T, and P_J.

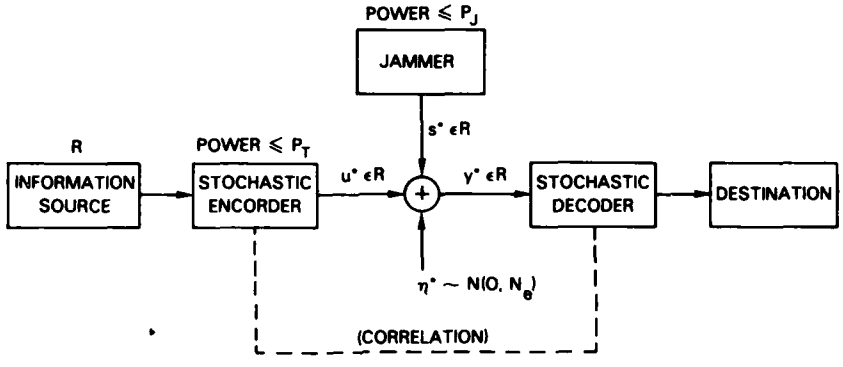


Fig. 1 — A Gaussian arbitrarily varying channel

We call the preceding model a *Gaussian Arbitrarily Varying Channel* (GAVC), since it is the continuous alphabet, Gaussian-noise-corrupted analog of the discrete, memoryless, *Arbitrarily Varying Channel* (AVC), introduced by Blackwell, Breiman and Thomasian [1] (see also Wolfowitz [2,3]). The study of discrete, memoryless AVCs has generated a substantial body of literature; much of this is summarized in Ref. 3, chapter 6.

By comparison, GAVCs have received considerably less attention. Blachman [4, 5], has obtained upper and lower bounds on the capacity of a GAVC (using the maximum probability of error concept) when the sequence $\{ s_i \}$ is allowed to be chosen with foreknowledge of the transmitter's codeword. Basar and Wu [6] have investigated the use of essentially the same channel, for a different source transmission problem in which the source is a discrete-time, memoryless Gaussian source and reliability is measured by mean-square distortion. Dobrushin [7] and later McEliece and Stark [8] have studied what might be called a *Gaussian compound channel* [2,3] that is similar to the GAVC except that the $\{ s_i \}$ is constrained to be a sequence of independent, identically distributed random variables.

The practical significance of the GAVC is seen as follows. One may view the sequence $\{ s_i \}$ as selected by an intelligent and unpredictable adversary, namely the *jammer*, whose intent is to disrupt the transmission of the sequence $\{ u_i \}$ as much as possible. The jammer, like the transmitter, is subject to the natural constraint of finite power but is otherwise free to generate any signal he chooses.

Manuscript approved February 13, 1986.

In this report, we study four GAVCs corresponding to two different types of power constraints (peak and average) on the transmitted codeword and on the jamming sequence. Our main results are coding theorems, one for each pair of constraints, characterizing the asymptotic reliability that can be achieved by optimum random codes on these channels. We say "asymptotic reliability" rather than capacity because, as we shall find, these channels generally have no capacity, per se.

2. DEFINITIONS AND RESULTS

A *codeword* of length n for the GAVC is a sequence of n real numbers selected by the transmitter, say $\mathbf{u} = (u_1, \ldots, u_n)$. Similarly, a *jamming sequence* of length n, denoted by $\mathbf{s} = (s_1, \ldots, s_n)$, is a sequence of n real numbers selected by the jammer. These sequences may be thought of geometrically as points in n-dimensional Euclidean space ($\mathbf{R}^n$). With this interpretation, the output of the GAVC corresponding to the codeword $\mathbf{u}$ and the jamming sequence $\mathbf{s}$ is

$$\mathbf{y}^* = \mathbf{u} + \eta_e^* + \mathbf{s}, \tag{2.1}$$

where η_e^* denotes an n-vector of independent, identically distributed (i.i.d.) $N(0, N_e)$ random variables.†

An *(n, M) block code*, C_n, is a system‡

$$C_n = \{ (\mathbf{u}_1, D_1), \ldots, (\mathbf{u}_M, D_M) \}, \tag{2.2}$$

where $\{\mathbf{u}_i\}_{i=1}^{M}$ are codewords of length n, and $\{D_i\}_{i=1}^{M}$ are disjoint (Borel) subsets of $\mathbf{R}^n$, called *decoding sets*. This code may be interpreted as a means of transmitting an integer message from the set $\{1, \ldots, M\}$ to the receiver using the GAVC. To send the number $1 \leqslant i \leqslant M$, the transmitter sends the codeword $\mathbf{u}_i$. At the receiving end, if the received sequence $\mathbf{y}^*$ lies in the set D_i, the receiver infers (perhaps incorrectly) that the transmitted message was i; otherwise, if $\mathbf{y}^*$ is exterior to each decoding set, the receiver draws no conclusion about the transmitted message.

We are interested in the problem of transmitting the output of a given information source, generating R bits per second, over the GAVC with minimum error probability (to be defined). The goal of the transmitter is to construct a block coding system of length n that suffers an error probability no greater than this minimum, regardless of the jamming sequence $\mathbf{s}$. The goal of the jammer is to inflict the largest possible error probability on any code chosen by the transmitter by an appropriate choice of $\mathbf{s}$. For the transmitter, a *strategy* to accomplish this goal consists of an $(n, 2^{nR})$ code; a strategy for the jammer is a jamming sequence of length n.

We allow both transmitter and jammer the additional flexibility of being able to choose their respective strategies *randomly*. Accordingly, we define an *(n, M) random (block) code*,

$$C_n^* = \{ (\mathbf{u}_1^*, D_1^*), \ldots, (\mathbf{u}_M^*, D_M^*) \}, \tag{2.3}$$

to be an (n, M) code-valued random variable that satisfies the obvious measurability requirements. A *(random) jamming sequence* of length n, with the obvious definition, is denoted by $\mathbf{s}^*$.

Clearly, if no further restrictions are imposed on the random codes and jamming sequences, the problem has an uninteresting solution. The error probability of any fixed, positive rate, random code can be made arbitrarily close to one by letting $\mathbf{s}^*$ be memoryless, zero-mean, Gaussian noise of arbitrarily large variance (or power). In practice, however, there will be other restrictions that prevent such

†Throughout this report, except where otherwise indicated, asterisks are used as superscripts to denote random variables, bold lower case letters indicate vectors (or vector-valued mappings) in $\mathbf{R}^n$, and $N(\mu, \sigma^2)$ denotes a Gaussian distribution with mean μ and variance σ^2

‡We extend this definition to nonintegral M as follows: By an *(n, M)* code we mean an (n, M') code where M' is the smallest integer greater than or equal to M.

trivial solutions. An interesting and natural restriction to investigate is that of placing some kind of *power constraint* on the codewords and the jamming sequences. In this report, we consider two types of power constraints: *peak* and *average*. We say that C_n^* satisfies a *peak input power constraint* (PI) if each codeword lies on or within an n-dimensional sphere (*n-sphere*) of radius $\sqrt{nP_T}$ almost surely (a.s.), i.e., if for each $1 \leqslant i \leqslant M$, the codeword $\mathbf{u}_i^* = (u_{i1}^*, \ldots, u_{in}^*)$ satisfies

$$\frac{1}{n} \sum_{j=1}^{n} u_{ij}^{*2} \leqslant P_T \quad \text{(a.s.)}. \tag{2.4}$$

This code satisfies an *average input power constraint* (AI) if the expected power averaged over all codewords is at most P_T; i.e., if

$$\mathbf{E}\left\{ \frac{1}{nM} \sum_{j=1}^{M} \sum_{i=1}^{n} u_{ij}^{*2} \right\} \leqslant P_T, \tag{2.5}$$

where $\mathbf{E}\{\,.\,\}$ denotes mathematical expectation. We also define two similar power constraints on the random jamming sequence $\mathbf{s}^*$. We say that $\mathbf{s}^*$ satisfies a *peak jamming power constraint* (PJ) if

$$\frac{1}{n} \sum_{i=1}^{n} s_i^{*2} \leqslant P_J \quad \text{(a.s.)} \tag{2.6}$$

and an *average jamming power constraint* (AJ) if

$$\mathbf{E}\left\{ \frac{1}{n} \sum_{i=1}^{n} s_i^{*2} \right\} \leqslant P_J. \tag{2.7}$$

There are two input power constraints (PI or AI) and two jamming power constraints (PJ or AJ), and so there are four possible combinations of transmitter and jammer power constraints to consider. We adopt a simple binary nomenclature to describe each case. In the sequel, when we speak of the GAVC A | B, we mean the GAVC with input power constraint A (= PI or AI), and jamming power constraint B (= PJ or AJ).

We now specify what is meant by the "error probability" of the code C_n^*. Given a code C_n^* on the GAVC A | B and the jamming sequence $\mathbf{s}^*$, we can in principle calculate the (maximum) probability of error:

$$\lambda(C_n^*, \mathbf{s}^*) \equiv \max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \eta_c^* + \mathbf{s}^* \in \bar{D}_i^*\}, \tag{2.8}$$

where $\bar{D}_i^*$ denotes $\mathbf{R}^n - D_i^*$. However, $\mathbf{s}^*$ is not known in advance to the transmitter and may change from one block to the next in an unpredictable and arbitrary way, subject only to the power constraint B. The smallest error probability *guaranteed* to be achievable by the code C_n^* is the supremum of Eq. (2.8) over all B-admissible $\mathbf{s}^*$. Therefore we define the error probability of the code C_n^* by

$$\lambda^{PJ}(C_n^*) = \sup_{\mathbf{s}^*} \lambda(C_n^*, \mathbf{s}^*), \tag{2.9}$$

where the supremum is performed over all B-admissible $\mathbf{s}^*$.

We now ask: For a given source rate R and constraint pair A | B, what is the smallest error probability, $\lambda^B(C_n^*)$, that can be achieved by any (n, M) random code C_n^* that satisfies constraint A, when $M \geq 2^{nR}$ and n is large? Clearly this error probability depends on both the rate R and the constraints A | B. Accordingly, we say that a pair (R, λ), where $R \geq 0$ and $0 \leq \lambda < 1$, is achievable for the case A | B (*achievable* A | B) if for all $\epsilon > 0$ there exists, for all n sufficiently large, an (n, M) random code C_n^* satisfying constraint A, so that

$$\log_2 M \geq n(R - \epsilon) \tag{2.10}$$

and

$$\lambda^B(C_n^*) \leq \lambda + \epsilon. \tag{2.11}$$

Let $\mathbf{R}_{A|B}$ denote the set of all achievable pairs (R, λ) for the GAVC A | B.

Note that if a certain pair (R, λ) is achievable A | B, then all pairs (R', λ'), such that $R' \leq R$ and $\lambda' \geq \lambda$, are also achievable A | B. Consequently, $\mathbf{R}_{A|B}$ must be of the form

$$\mathbf{R}_{A|B} = \{(R, \lambda) \mid 0 \leq R \leq C_{A|B}(\lambda),\ 0 \leq \lambda < 1\} \tag{2.12}$$

where $C_{A|B}(\lambda)$ is a monotone increasing function of λ. Thus, to characterize $\mathbf{R}_{A|B}$ it suffices to determine $C_{A|B}(\lambda)$.

The function $C_{A|B}(\lambda)$ is called the λ-*capacity* of the channel (cf. Csiszár and Körner [3] and Wolfowitz [2]). It can be interpreted as the largest rate of transmission that can be achieved by a code with error probability no greater than λ, for large n. If $C_{A|B}(\lambda)$ is equal to a constant on $0 \leq \lambda < 1$, say $C_{A|B}$, the latter is called the *capacity* of the channel; otherwise, if $C_{A|B}(\lambda)$ is *not* constant, we say that no capacity exists.† Most simple channel models that arise in information theory have a capacity. In this report, we show that certain GAVCs generally have no capacity; i.e., $C_{A|B}(\lambda)$ is not constant. This interesting and somewhat surprising fact distinguishes GAVCs from discrete AVCs: Blackwell, Breiman, and Thomasian [1] have shown that the latter *always* possess a (random coding) capacity.

Recall that our objective is to determine the minimum error probability suffered by large block-length random codes of rate R when used on the GAVC A | B. Define this error probability by

$$\lambda^{A|B}(R) \equiv \limsup_{n \to \infty} \inf_{C_n^*} \lambda^B(C_n^*), \tag{2.13}$$

where the infimum is over all A-admissible $(n, 2^{nR})$ random codes. It is easy to see that the relationship between $\lambda^{A|B}(R)$ and $C_{A|B}(\lambda)$ is

$$\lambda^{A|B}(R) = \min\{0 \leq \lambda \leq 1 \mid C_{A|B}(\lambda) \geq R \text{ or } \lambda = 1\}. \tag{2.14}$$

Although it clearly provides the same information about $\mathbf{R}_{A|B}$ that $C_{A|B}(\lambda)$ does, $\lambda^{A|B}(R)$ is often easier to interpret.

We now present four theorems that characterize $C_{A|B}(\lambda)$ for each pair of constraints A | B, the proofs of which are provided in the next section. We first consider the case in which both transmitter and jammer are constrained in peak power, i.e., the GAVC PI | PJ. This channel actually has a capacity that is given by the following familiar formula.

†An alternative (e.g. Csiszár and Körner [3]) definition of capacity (which always exists) is

$$C_{A|B} \equiv \lim_{\lambda \to 0^+} C_{A|B}(\lambda).$$

Our definition is that of Wolfowitz [2].

Theorem 1: For the GAVC PI | PJ, a (random coding) capacity exists and is given by

$$C_{PI\,|\,PJ}(\lambda) = C_{PI\,|\,PJ} = \frac{1}{2}\log_2\left(1 + \frac{P_T}{N_e + P_J}\right) \tag{2.15}$$

for all $0 \leqslant \lambda < 1$.

Remark: Blachman ([4], p. 53, Eq. 10) states (without proof) a similar result.

It is interesting to note that $C_{PI\,|\,PJ}$ is identical to the capacity formula of the memoryless, Gaussian channel that would be formed if the jammer transmitted a sequence of i.i.d. $N(0,P_J)$ random variables (eg. Wolfowitz [2], Theorem 9.2.1).†‡ We conclude, for the GAVC PI | PJ, that an intelligent jammer, regardless of how he distributes his power, can do no more harm (in the sense of reducing the achievable region) than Gaussian noise of the same power.

We now change the jamming power constraint from PJ to AJ (i.e., GAVC PI | AJ) and ask whether the above conclusion is still valid. Since bounds on average power are *weaker* than those on peak power, it is obvious that $\mathbf{R}_{PI\,|\,AJ}$ is a subset of $\mathbf{R}_{PI\,|\,PJ}$. However, as the next theorem demonstrates, this inclusion is strict. In fact, we find, for this and all remaining cases in which either transmitter or jammer or both are subject to *average* power constraints, that *no capacity exists*, i.e., only λ-capacities are found.

Theorem 2: For the GAVC with constraints PI | AJ the (random coding) λ-capacity is

$$C_{PI\,|\,AJ}(\lambda) = \frac{1}{2}\log_2\left(1 + \frac{P_T}{N_e + P_J/\lambda}\right) \tag{2.16}$$

for all $0 \leqslant \lambda < 1$.

Remark: $C_{PI\,|\,AJ}(0)$ is interpreted as 0.

Observe that the expression for $C_{PI\,|\,AJ}(\lambda)$ is identical to that of $C_{PI\,|\,PJ}$ except that the jamming power appears boosted by a factor that is the reciprocal of the tolerable error probability, λ. Some insight into this formula can be gained by stating the result in terms of the error probability suffered by codes of rate R. Theorem 2 states that, for increasing n, optimal $(n, 2^{nR})$ random codes satisfying PI suffer an error probability that approaches

$$\lambda^{PI\,|\,AJ}(R) = \begin{cases} \dfrac{(4^R - 1)P_J}{P_T - (4^R - 1)N_e} & R \leqslant C_{PI\,|\,AJ}(1) \\ 1, & R < C_{PI\,|\,AJ}(1) \end{cases} \tag{2.17}$$

against an AJ-constrained jammer.

The function $\lambda^{PI\,|\,AJ}(R)$ is increasing, positive whenever R is positive, and for small R becomes asymptotic to $2 \ln 2\ R\ P_J/P_T$. The region $\mathbf{R}_{PI\,|\,AJ}$ is sketched in Fig. 2. Apparently, a code can achieve high reliability (i.e., $\lambda^{AJ}(C_n^*) \approx 0$) only in the limit as R or P_J/P_t become vanishingly small. Evidently, *reliable communication is impossible at any positive source rate.*

†It is also the formula obtained by Dobrushin [7] for the capacity of the Gaussian *compound channel*.

‡Note that this Gaussian jamming sequence does not satisfy PJ. It is possible, however, to construct a jamming sequence that does satisfy PJ and that yields nearly the same capacity (cf. proof of Theorem 2).

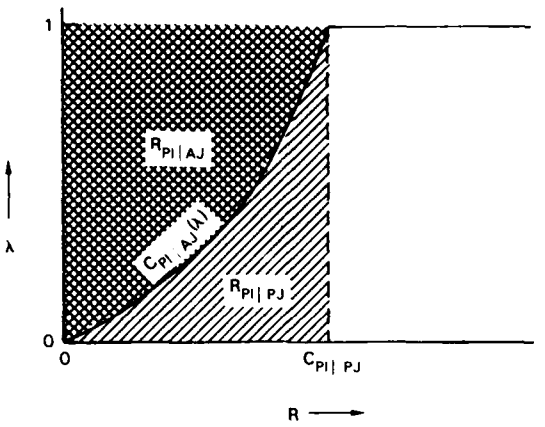


Fig. 2 — The achievable regions for GAVC PI | PJ and PI | AJ

We now sketch the basic idea behind Eq. (2.17) (or equivalently, Theorem 2); a detailed proof follows in Section 3. Let C_n^* be any PI-admissible random code of rate R. Suppose the jammer transmits only jamming sequences $\mathbf{s}^*$ consisting of i.i.d. sequences of $N(0, P^*)$ random variables, where P^* is a nonnegative random variable that satisfies $EP^* \leqslant P_J$, so that $\mathbf{s}^*$ satisfies AJ. (Clearly, this restriction can only *increase* the achievable region.) With this restriction, the channel "seen" by the transmitter is a discrete-time, Gaussian channel with (unknown) noise power $N_e + P^*$. According to the coding theorem and strong converse for this channel (e.g. Wolfowitz [2], Theorems 9.2.1-2), if

$$R < \frac{1}{2} \log_2 \left(1 + \frac{P_T}{N_e + P^*} \right)$$

and n is large, then $\lambda^{AJ}(C_n^*) \approx 0$ is possible; however, if

$$R > \frac{1}{2} \log_2 \left(1 + \frac{P_T}{N_e + P^*} \right),$$

then $\lambda^{AJ}(C_n^*) \approx 1$ is certain. The jammer must therefore choose

$$P^* \geqslant \frac{P_T}{(4^R - 1)} - N_e$$

to be guaranteed an appreciable error probability, and this power is sufficient to yield an error probability of unity. Therefore, the best codes have error probability that approximates the probability of this event

$$\lambda^{AJ}(C_n^*) \approx Pr \left\{ P^* \geqslant \frac{P_T}{(4^R - 1)} - N_e \right\}.$$

Finally, the right-hand expression above takes on a maximum value of $\lambda^{PI|AJ}(R)$ when P^* is chosen so that

$$Pr \left\{ P^* \approx \frac{P_T}{(4^R - 1)} - N_e \right\} = 1 - Pr\{P^* = 0\} = \lambda^{PI|AJ}(R).$$

It follows that $\lambda^{AJ}(C_n^*)$ is not less than $\lambda^{PI|AJ}(R)$ for large n.

Although we have allowed the jammer foreknowledge of the statistics of the transmitter's random code when selecting a jamming sequence (cf. Eq. (2.9)), it turns out that this knowledge is unnecessary. Remarkably, the jamming sequence above does not depend on the detailed structure of the code, but only on the blocklength n, the source rate R, and the parameters P_I, P_J, and N_c. Also interesting is that this jamming sequence is essentially a *pulsed strategy* (i.e., either "off" or "on" with high peak power). Memoryless, pulsed jamming sequences have been shown to maximize the error probability of certain uncoded modulation systems, such as BPSK (e.g. Simon et al. [9]). Theorem 2 shows that pulsed jamming sequences *with memory* play a similar role for random block codes on the GAVC.

We have seen from Theorem 2 that an average-power-limited jammer has a tremendous advantage against a peak-power-limited transmitter; in fact, reliable communication is impossible in this case. It is interesting to turn the tables and ask whether the transmitter might similarly gain by varying codeword power against a peak-power-limited jammer, as in the case AI | PJ. The next theorem shows that little advantage will be gained.

Theorem 3: For the GAVC with constraints AI | PJ, the (random coding) λ-capacity is

$$C_{AI|PJ}(\lambda) = \frac{1}{2}\log_2\left(1 + \frac{P_I/(1-\lambda)}{N_c + P_J}\right) \tag{2.18}$$

for all $0 \leqslant \lambda < 1$.

The corresponding achievable region is sketched in Fig. 3. We see that if a high error probability can be tolerated, the allowable coding rate is much improved; however, at low error probabilities $C_{AI|PJ}(\lambda)$ approaches $C_{PI|PJ}$, and the improvements are negligible. As in the other cases, we can state the result in terms of error probabilities: Optimal AI-admissible $(n, 2^{nR})$ random codes suffer an error probability that, for large n, approaches

$$\lambda^{AI|PJ}(R) = \begin{cases} 0, & R \leqslant C_{AI|PJ}(0) \\ 1 - \dfrac{P_I}{(4^R - 1)(N_c + P_J)}, & R > C_{AI|PJ}(0). \end{cases} \tag{2.19}$$

Thus the rates at which reliable communication can occur are the same as the case PI | PJ. Clearly, codeword power variation offers little improvement to the transmitter.

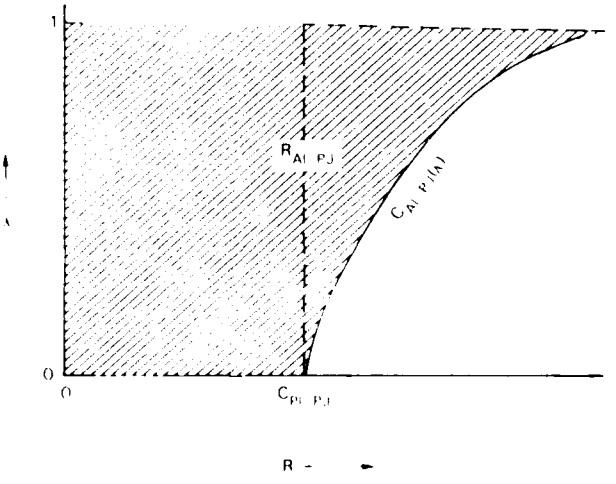


Fig. 3 — The achievable region for GAVC AI | PJ

We now consider the GAVC AI | AJ. As Theorem 3 shows, the additional flexibility offered by the power constraint AI is relatively useless against a peak-power-limited jammer. We now ask if the transmitter might at least reduce the gain of the average-power-limited jammer compared with the GAVC PI AJ. The next theorem shows that some limited improvement is made.

Theorem 4: For the GAVC with constraints AI | AJ the (random coding) λ-capacity, for $N_e > 0$, is given by

$$C_{AI|AJ}(\lambda) = \begin{cases} \frac{1}{2}\log_2\left(1 + \frac{P_T}{N_e + P_J/2\lambda}\right), & 0 \leqslant \lambda \leqslant \lambda_c \\ \frac{1}{2}\log_2\left(1 + \frac{P_T(1-2\lambda_c)}{(1-\lambda)N_e}\right), & \lambda_c \leqslant \lambda < 1 \end{cases} \tag{2.20a}$$

where

$$\lambda_c \equiv \frac{P_J}{2N_e}\left(\sqrt{1 + \frac{2N_e}{P_J}} - 1\right)$$

and in the case $N_e = 0$ by

$$C_{AI|AJ}(\lambda) = \begin{cases} \frac{1}{2}\log_2\left(1 + \frac{2\lambda P_T}{P_J}\right), & 0 \leqslant \lambda < \frac{1}{2} \\ \frac{1}{2}\log_2\left(1 + \frac{P_T}{2(1-\lambda)P_J}\right), & \frac{1}{2} \leqslant \lambda < 1 \end{cases} \tag{2.20b}$$

Remark: Equation (2.20a) tends continuously to Eq. (2.20b) as $N_e \to 0$.

The corresponding achievable region is sketched in Fig. 4, with $C_{PI|PJ}$, $C_{PI|AJ}(\lambda)$, and $C_{AI|PJ}(\lambda)$ included for comparison. Optimal $(n, 2^{nR})$ random codes satisfying AI must then, as n grows large, suffer an error probability that approaches

$$\lambda^{AI|AJ}(R) = \begin{cases} \frac{P_J(4^R - 1)}{2(P_T - (4^R - 1)N_e)}, & R \leqslant C_{AI|AJ}(\lambda_c) \\ 1 - \frac{P_T(1-2\lambda_c)}{(4^R - 1)N_e}, & R > C_{AI|AJ}(\lambda_c) \end{cases} \tag{2.21a}$$

when $N_e > 0$, and

$$\lambda^{AI|AJ}(R) = \begin{cases} \frac{P_J(4^R - 1)}{2P_T}, & R \leqslant \frac{1}{2}\log_2\left(1 + \frac{P_T}{P_J}\right) \\ 1 - \frac{P_T}{2(4^R - 1)P_J}, & R > \frac{1}{2}\log_2\left(1 + \frac{P_T}{P_J}\right) \end{cases} \tag{2.21b}$$

when $N_e = 0$.

For $R < C_{AI|AJ}(\lambda_c)$, observe that the error probability is half of that of GAVC PI | AJ; however, when $R > C_{AI|AJ}(\lambda_c)$ the probability of being *correct* $(= 1 - \lambda^{AJ}(C^*_n))$ is $(1 - 2\lambda_c)$ of that in the case AI | PJ. $C_{AI|AJ}(\lambda)$ is therefore a compromise between $C_{PI|AJ}(\lambda)$ and $C_{AI|PJ}(\lambda)$. As in the case PI AJ, the error probability can be made small only by making R or P_J/P_T small.

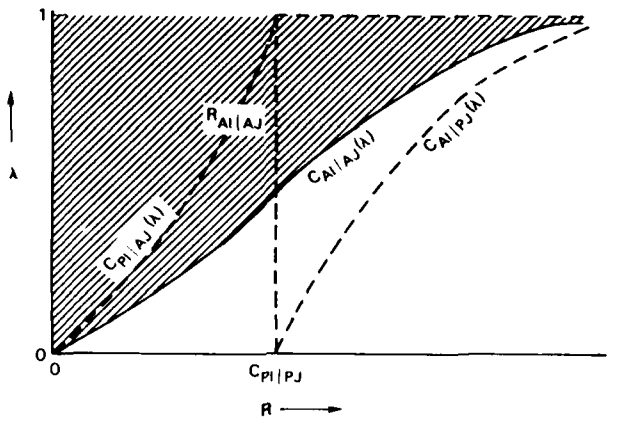


Fig. 4 — The achievable region for GAVC AI | AJ (with all other λ-capacities included for comparison)

An intuitive justification of Eq. (2.21a) is given here (a rigorous proof is given in Section 3). Suppose, as before, the jammer transmits only i.i.d. sequences of $N(0, P_2^*)$ random variables, say s, where P_2^* is a nonnegative random variable that satisfies $\mathbf{E}P_2^* \leqslant P_J$. The transmitter constructs a random code C_n^* in the following way: He first selects a random code $\bar{C}_n^*$ of rate R whose average power is no greater than unity, i.e.,

$$\mathbf{E}\left\{ \frac{1}{nM} \sum_{j=1}^{M} \sum_{i=1}^{n} u_{ij}^{*2} \right\} \leqslant 1,$$

and then, to form C_n^*, he multiplies each codeword in $\bar{C}_n^*$ by $\sqrt{P_1^*}$, where P_1^* is an independent nonnegative random variable satisfying $\mathbf{E}P_1^* \leqslant P_T$. The performance of this code against $\mathbf{s}^*$ is a function of the signal-to-noise ratio $P_1^*/(P_2^* + N_e)$. As in the earlier argument following Theorem 2, if

$$\frac{P_1^*}{P_2^* + N_e} > (4^R - 1),$$

then $\lambda(C_n^*, \mathbf{s}^*)$ can be small; however, if

$$\frac{P_1^*}{P_2^* + N_e} < (4^R - 1),$$

then it is certainly true that $\lambda(C_n^*, \mathbf{s}^*) \approx 1$. Therefore, for the best choice of $\bar{C}_n^*$, we have for large n

$$\lambda(C_n^*, \mathbf{s}^*) \approx Pr\{ P_1^* < (4^R - 1)(P_2^* + N_e) \}. \tag{2.22}$$

The optimum error probability thus depends only on the power distribution of the transmitter and jammer. Naturally, the transmitter wants to minimize Eq. (2.22) with an appropriate choice of P_1^*, and the jammer wants to maximize it by an effective choice of P_2^*. Therefore, an optimal code suffers the error probability

$$\lambda^{AJ}(C_n^*) \approx \max_{P_1^*:\mathbf{E}P_1^* \leqslant P_T} \min_{P_2^*:\mathbf{E}P_2^* \leqslant P_J} Pr\{ P_1^* < (4^R - 1)(P_2^* + N_e) \}.$$

It can be shown (cf. proof of Theorem 4) that the right-hand side of this equation is equal to $\lambda^{AI|AJ}(R)$.

Finally, consider the coding problems that result from the imposition of *multiple* constraints. Suppose our code must satisfy some constraint, say A, for some constant P_T, and another constraint A' for some constant $P_T' \neq P_T$. Denote this joint constraint by AA'. Similarly, one may define a double constraint, BB', on jamming vectors. It is easily checked that the achievable regions for these more complex coding problems can be constructed from the regions defined by Theorems 1 to 4 according to the following simple rules:†

$$\mathbf{R}_{AA'|B} = \mathbf{R}_{A|B} \cap \mathbf{R}_{A'|B} \tag{2.23a}$$

$$\mathbf{R}_{A|BB'} = \mathbf{R}_{A|B} \cup \mathbf{R}_{A|B'}, \tag{2.23b}$$

or, in terms of λ-capacities:

$$C_{AA'|B}(\lambda) = \min\{C_{A|B}(\lambda), C_{A'|B}(\lambda)\} \tag{2.24a}$$

$$C_{A|BB'}(\lambda) = \max\{C_{A|B}(\lambda), C_{A|B'}(\lambda)\}. \tag{2.24b}$$

3. THE PROOFS OF THEOREMS 1 TO 4:

For any input power constraint A, and jamming power constraint B, define the region

$$\hat{\mathbf{R}}_{A|B} \equiv \{(R,\lambda) \mid 0 \leqslant R \leqslant \hat{C}_{A|B}(\lambda), 0 \leqslant \lambda < 1\},$$

where $\hat{C}_{A|B}(\lambda)$ is the formula given in the theorem of Section 2 corresponding to the constraints A | B. Our goal in this section is to prove that

$$\mathbf{R}_{A|B} = \hat{\mathbf{R}}_{A|B},$$

for each pair of constraints A | B. Each proof will consist of two parts: a *forward part*

$$\text{(a)}: \mathbf{R}_{A|B} \supset \hat{\mathbf{R}}_{A|B},$$

and a *strong converse*

$$\text{(b)}: \mathbf{R}_{A|B} \subset \hat{\mathbf{R}}_{A|B}.$$

At this point, it is convenient to present some definitions and results that we use in the proofs below. By the *standard (n , M) random code*, we mean a random code

$$\hat{C}^*_n \equiv \{(\mathbf{v}^*_1, A^*_1), \ldots, (\mathbf{v}^*_M, A^*_M)\}, \tag{3.1}$$

constructed in the following way.

(1) The M random codewords, $\{\mathbf{v}^*_1, \ldots, \mathbf{v}^*_M\}$, are a collection of mutually independent, random n-vectors, each of which is uniformly distributed on the n-sphere of radius $\sqrt{n}$; i.e., the probability that $\mathbf{v}^*_i$ lies within a certain region on the surface of this n-sphere is proportional to the surface area (or equivalently, solid angle) of this region.

(2) The random decoding sets, $\{A^*_i\}_{i=1}^{M}$, are defined by a *strict minimum Euclidean distance* rule, viz.,

$$A^*_i \equiv \{y \in \mathbf{R}^n \mid |\mathbf{y}-\mathbf{v}^*_i| < |\mathbf{y}-\mathbf{v}^*_k|, \text{for all } k \neq i, 1 \leqslant k \leqslant M\}, \tag{3.2}$$

† It is unknown whether the region $\mathbf{R}_{AA'|BB'}$ can be similarly decomposed

where $|\cdot|$ denotes the usual Euclidian norm on $\mathbf{R}^n$. If a tie occurs, the receiver draws no conclusion about the transmitted message (and hence an error occurs).†

We make several observations about the random code, $\hat{C}_n^*$. First, the codewords of $\hat{C}_n^*$ are clearly PI-admissible for $P_1 = 1$; in fact, Eq. (2.4) is satisfied with equality (with probability one). Second, since all codewords have equal length (or power), each decoding set in Eq. (3.2) is a "flat-sided" cone with vertex at the origin. It follows that the sets $\{A_i^*\}_{i=1}^M$ are also minimum distance decoding sets for every codeword set of the form $\{\sqrt{P}\,\mathbf{v}_1^*, \ldots, \sqrt{P}\,\mathbf{v}_M^*\}$, where $P > 0$. Third, Shannon [10] has considered the use of this random code on the discrete-time, additive Gaussian noise channel and has obtained the following result: There exists functions, say $K(R,P)$ and (R,P), both positive so long as

$$R \equiv \frac{1}{n}\log_2 M < \frac{1}{2}\log_2(1+P), \tag{3.3}$$

such that‡

$$Pr\{\sqrt{P}\,\mathbf{v}_i^* + \eta^* \in \bar{A}_i^*\} \leqslant K(R,P)\exp\{-nE(R,P)\} \tag{3.4}$$

holds for all $1 \leqslant i \leqslant M$ and $n \geqslant 1$, where, here and throughout this section, η^* denotes a vector of i.i.d. $N(0,1)$ random variables. Furthermore, $K(R,P)$ and $E(R,P)$ can be selected so that

(a) $K(\cdot,P)$, $-E(\cdot,P)$ are increasing, and (3.5a)

(b) $K(R,\cdot)$, $-E(R,\cdot)$ are decreasing (3.5b)

for all R and P satisfying Eq. (3.3). Finally, $\hat{C}_n^*$ has the useful properties summarized in the following lemma whose proof is contained in Appendix A.

Lemma 1: Let $\hat{C}_n^*$ be the standard random code (Eq. (3.1)); let $\mathbf{s}$ be any n-vector, and let l and $\hat{l}$ be any pair of real numbers satisfying $l \geqslant \hat{l} \geqslant 0$. Let ω^* be a random variable that is uniformly distributed on the unit n-sphere, and that is independent of the codewords $\{\mathbf{v}_1^*, \ldots, \mathbf{v}_M^*\}$. Then

$$(a)\ Pr\{\mathbf{v}_1^* + \eta_c^* + \mathbf{s} \in \bar{A}_1^*\} = Pr\{\mathbf{v}_1^* + \eta_c^* + |\mathbf{s}|\omega^* \in \bar{A}_1^*\},$$

$$(b)\ Pr\{\mathbf{v}_1^* + \eta_c^* + \hat{l}\omega^* \in \bar{A}_1^*\} \leqslant Pr\{\mathbf{v}_1^* + \eta_c^* + l\omega^* \in \bar{A}_1^*\}.$$

Remark: Lemma 1, part (a) states that $Pr\{\mathbf{v}_1^* + \eta_c^* + \mathbf{s} \in \bar{A}_1^*\}$ depends only on the *magnitude* of $\mathbf{s}$, and not on its orientation; part (b) implies that it is an *increasing* function of this magnitude.

A second useful lemma is given below; its proof is contained in Appendix B.

Lemma 2: Let $\{\eta_i^*\}_{i=1}^\infty$ be a sequence of i.i.d. random variables with common marginal distribution $N(0,1)$. Then for all $0 \leqslant \epsilon < 1$,

$$\text{(a): } Pr\left\{\left|\frac{1}{n}\sum_{i=1}^{n}\eta_i^{*2} - 1\right| \geqslant \epsilon\right\} \leqslant \exp\left\{-\frac{n\epsilon^2}{12}\right\}$$

† We note that the decoding sets $\{A_i^*\}_{i=1}^M$ may be suboptimal (in the minimax sense) decision regions for the loss functions $\lambda^{PJ}(\hat{C}_n^*)$ and $\lambda^{AJ}(\hat{C}_n^*)$. For proving coding theorems this will not matter: in the forward part of the proofs we can certainly bound the error probability of the optimal decoders above by that obtained using suboptimal decoding sets; in the converse part, we can bound the worst-case error probability below by that obtained using (block) pulsed, Gaussian jamming signals, for which the sets, $\{A_i^*\}_{i=1}^M$, are a uniformly most powerful decision rule

‡ We have presented Shannon's result in a form that is different from the original statement in Ref. 10, but which is convenient for the proofs of the present section. Our form can be obtained from Shannon's "firm" upper bound in Ref. 10 by making the substitution indicated in the footnote to page 16 of Gallager [11] and simplifying the resulting bound

for all $n \geq n_0(\epsilon)$, where $n_0(\epsilon)$ is a bounded function of ϵ alone, and†

$$\text{(b): } Pr\left\{ \frac{1}{n} \sum_{i=1}^{n} \eta_i^{*2} \geq 1 \right\} \geq Pr\{ \eta_1^2 \geq 1 \} \geq \frac{1}{4},$$

for all $n \geq 1$.

We also require an Arimoto-style strong converse [12] for the discrete-time, additive Gaussian noise channel with peak input power constraint and the *average* probability of error concept. Let

$$C_n^* \equiv \{ (\mathbf{u}_1^*, D_1^*), \ldots, (\mathbf{u}_M^*, D_M^*) \}$$

be any PI-admissible (n, M) random code with $P_T = P$. There exist functions, say $K'(R, P)$ and $E'(R, P)$, which are both positive whenever

$$R \equiv \frac{1}{n} \log_2 M > \frac{1}{2} \log_2 (1 + P), \tag{3.6}$$

such that

$$\frac{1}{M} \sum_{i=1}^{M} Pr\{ \mathbf{u}_i^* + \eta^* \in \bar{D}_i^* \} \geq 1 - K'(R, P) \exp\{ -nE'(R, P) \} \tag{3.7}$$

holds for all $n \geq 1$. (Note that any lower bound on the average error probability is *a fortiori* a lower bound to the maximum probability of error.) Furthermore, $K'(R, P)$ and $E'(R, P)$ can be selected so that

(a) $K'(\cdot, P)$, $-E'(\cdot, P)$ are increasing, and (3.8a)

(b) $K'(R, \cdot)$, $-E'(R, \cdot)$ are decreasing (3.8b)

for all R and P that satisfy Eq. (3.6). The proof of this result is very similar to the derivation in Section VI of Ref. 10; we therefore omit it.

We now present a Lemma that forms the kernel of the strong converses to Theorems 3 and 4. This Lemma is of independent interest because it gives a tight lower bound on the average error probability of any code when used on a Gaussian channel in terms of the code's power distribution.

Define for any $\mathbf{u} = (u_1, \ldots, u_n) \in \mathbf{R}^n$ the quantity

$$P(\mathbf{u}) \equiv \frac{1}{n} \sum_{i=1}^{n} u_i^2, \tag{3.9}$$

and for any random code C_n^*, let $U^*(C_n^*)$ be the random variable that is uniformly distributed on the set $\{ \mathbf{u}_1^*, \ldots, \mathbf{u}_M^* \}$ of codewords of C_n^*.

Lemma 3: Let C_n^* be any (n, M) random code and J^* be any nonnegative random variable that is independent of C_n^*. Then for all $\epsilon > 0$ the following holds:

$$\frac{1}{M} \sum_{i=1}^{M} Pr\{ \mathbf{u}_i^* + \eta_e^* + \sqrt{J^* \eta^*} \in \bar{D}_i^* \}$$

$$\geq Pr\{ P(U(C_n^*)) < (4^{R - 2\epsilon} - 1)(N_e + J^*) \} - \gamma_n(\epsilon), \tag{3.10}$$

†By the Central Limit Theorem, the left-most expression in Lemma 2(b) approximates 1/2 for large n.

where

$$\gamma_n(\epsilon) \equiv K'(R-\epsilon, 4^{R-2\epsilon}-1)\exp\{-nE'(R-\epsilon, 4^{R-2\epsilon}-1)\} - 2^{-n\epsilon}. \tag{3.11}$$

Remarks: Observe that $\gamma_n(\epsilon)$ depends *only* on n, ϵ, and R and is independent of the random code and the jamming power. Also, for all $\epsilon > 0$, $\gamma_n(\epsilon) \to 0$ exponentially fast.

Proof of Lemma 3: To prove the lemma, fix $\epsilon > 0$, and let $C_n \equiv \{(\mathbf{u}_1, D_1), \ldots, (\mathbf{u}_M, D_M)\}$ be any realization of C_n^*. Define the set

$$S_\epsilon(C_n, J) \equiv \{1 \leqslant i \leqslant M \mid P(\mathbf{u}_i) < (4^{R-2\epsilon}-1)(N_e + J)\}, \tag{3.12}$$

and further define†

$$N_\epsilon(C_n, J) \equiv \#S_\epsilon(C_n, J). \tag{3.13}$$

It is immediate that

$$E\{N_\epsilon(C_n^*, J^*)\} = M\, Pr\{P(U^*(C_n^*)) < (4^{R-2\epsilon}-1)(N_e + J^*)\}. \tag{3.14}$$

The *average* error probability of that subcode of C_n that consists of those codewords with indexes in $S_\epsilon(C_n, J)$ can be bounded below by the strong converse (cf. Eq. (3.7)) for the Gaussian channel ‡

$$\frac{1}{N_\epsilon(C_n, J)} \sum_{i \in S_\epsilon(C_n, J)} Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{J}\,\eta^* \in \bar{D}_i^* \mid C_n^* = C_n\}$$
$$\geqslant 1 - K'(R_n, 4^{R-2\epsilon}-1)\exp\{nE'(R_n, 4^{R-2\epsilon}-1)\} \tag{3.15}$$

provided that

$$R_n \equiv \frac{\log_2(N_\epsilon(C_n, J))}{n} > R - 2\epsilon. \tag{3.16}$$

In particular, the following holds for all C_n, J, ϵ, and R: §

$$\frac{1}{N_\epsilon(C_n, J)} \sum_{i \in S_\epsilon(C_n, J)} Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{J}\,\eta^* \in \bar{D}_i^* \mid C_n^* = C_n\}$$
$$\geqslant (1 - K'(R_n, 4^{R-2\epsilon}-1)\exp\{-nE'(R_n, 4^{R-2\epsilon}-1)\}\, 1_{\{R_n \mid R_n \geqslant R-\epsilon\}}(R_n)$$
$$\geqslant (1 - B_n(R, \epsilon))\, 1_{\{R_n \mid R_n \geqslant R-\epsilon\}}(R_n), \tag{3.17}$$

where

$$B_n(R, \epsilon) \equiv K'(R-\epsilon, 4^{R-2\epsilon}-1)\exp\{-nE'(R-\epsilon, 4^{R-2\epsilon}-1)\}.$$

† The quantity $\#A$ denotes the cardinality of the set A.

‡ We interpret the left-hand expression in Eq. (3.15) as zero if $N_\epsilon(C_n, J) = 0$.

§ $1_A(x) \equiv \begin{cases} 1 & x \in A \\ 0 & x \in \bar{A} \end{cases}$.

The last step above is a consequence of Eqs. (3.16) and (3.8a). Using Eq. (3.17), we obtain the desired lower bound to the average error probability of C_n:

$$\frac{1}{M}\sum_{i=1}^{M} Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{J}\ \eta^* \in \bar{D}_i^* \mid C_n^* = C_n\}$$

$$\geqslant \frac{1}{M}\sum_{i \in S_\epsilon(C_n, J)} Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{J}\ \eta^* \in \bar{D}_i^* \mid C_n^* = C_n\}$$

$$\geqslant \frac{N_\epsilon(C_n, J)}{M}\,(1 - B_n(R, \epsilon))\, 1_{\{R_n \mid R_n \geqslant R-\epsilon\}}(R_n)$$

$$= \frac{N_\epsilon(C_n, J)}{M} - \frac{N_\epsilon(C_n, J)}{M}\, B_n(R, \epsilon)\, 1_{\{R_n \mid R_n \geqslant R-\epsilon\}}(R_n)$$

$$- \frac{N_\epsilon(C_n, J)}{M}\, 1_{\{R_n \mid R_n < R-\epsilon\}}(R_n)$$

$$\geqslant \frac{N_\epsilon(C_n, J)}{M} - B_n(R, \epsilon) - 2^{n\epsilon}$$

$$\equiv \frac{N_\epsilon(C_n, J)}{M} - \gamma_n(\epsilon). \tag{3.18}$$

Averaging Eq. (3.18) over the distributions of C_n^* and J^* and using Eq. (3.14), we obtain Eq. (3.10), completing the proof.

Proof of Theorem 1:

(a): $\mathbf{R}_{PI \mid PJ} \supset \hat{\mathbf{R}}_{PI \mid PJ}$.

Let R, nonnegative, be given and set $M_n = \lfloor 2^{nR} \rfloor$.† Define a sequence of (n, M_n) random codes, say $\{C_n^*\}_{n=1}^{\infty}$, in the following way:

$$C_n^* = \{(\mathbf{u}_1^*, A_1^*), \ldots, (\mathbf{u}_{M_n}^*, A_{M_n}^*)\}, \tag{3.19}$$

where $\mathbf{u}_i^* = \sqrt{P_I}\ \mathbf{v}_i^*$, and $\{(\mathbf{v}_1^*, A_1^*), \ldots, (\mathbf{v}_{M_n}^*, A_{M_n}^*)\}$ is the standard (n, M_n) random code, defined in Eq. (3.1). It is easily verified that C_n^* satisfies PI for each $n \geqslant 1$. We further claim that if

$$R < C_{PI \mid PJ}, \tag{3.20}$$

then there is a positive sequence $\{\gamma_n\}_{n=1}^{\infty}$ such that

$$\lambda^{PJ}(C_n^*) \leqslant \gamma_n \tag{3.21}$$

and $\gamma_n \to 0$ as $n \to +\infty$. If true, this would clearly imply that any $R, \lambda)$ in $\hat{\mathbf{R}}_{PI \mid PJ}$ is achievable PI | PJ, and thus prove (a).

†$\lfloor x \rfloor$ denotes the integer such that $x - 1 < n \leq x$

To establish this claim, suppose that Eq. (3.20) is true; let ω^* be an independent random variable that is uniformly distributed on the unit n-sphere and define

$$\sigma_n(l) \equiv Pr\{\mathbf{u}_i^* + \eta_e^* + l\omega^* \in \bar{A}_i^*\} \tag{3.22}$$

for any real number $l \geq 0$. (Clearly, $\sigma_n(\cdot)$ does *not* depend on i.) Let $\mathbf{s}^*$ be any jamming sequence that satisfies PJ; i.e., $|\mathbf{s}^*| \leq \sqrt{nP_J}$, with probability one. The error probability incurred by $\mathbf{s}^*$ can be bounded in the following way:

$$Pr\{\mathbf{u}_i^* + \eta_e^* + \mathbf{s}^* \in \bar{A}_i^*\} \overset{(a)}{=} \mathbf{E}\,\sigma_n(|\mathbf{s}^*|) \overset{(b)}{\leq} \sigma_n(\sqrt{nP_J}). \tag{3.23}$$

The justification of these steps is as follows: (a) is a consequence of Lemma 1(a) and the definition of $\mathbf{u}_i^*$; (b) results from PJ and Lemma 1(b). Taking the supremum of Eq. (3.23) over all $1 \leq i \leq M$ and $\mathbf{s}^*$ satisfying PJ, we obtain the bound

$$\lambda^{PJ}(C_n^*) \leq \sigma_n(\sqrt{nP_J}). \tag{3.24}$$

It only remains to estimate the right-hand expression in Eq. (3.24); this is easily done by relating it to the error probability for the ordinary Gaussian channel. Let $\sqrt{P_J}\eta^*$ denote a vector of i.i.d. $N(0,P_J)$ random variables, and let $f(\cdot)$ denote the probability density function of the random variable $m^* \equiv \sqrt{P_J}\,|\eta^*|$. It is easy to show that

$$Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{P_J}\,\eta^* \in \bar{A}_i^*\} = \int_0^\infty \sigma_n(l) f(l)\, dl. \tag{3.25}$$

Using Lemma 1(b) again, we find

$$\sigma_n(\sqrt{nP_J}) \leq \frac{\int_{\sqrt{nP_J}}^\infty \sigma_n(l) f(l)\, dl}{\int_{\sqrt{nP_J}}^\infty f(l)\, dl} \leq \frac{Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{P_J}\,\eta^* \in \bar{A}_i^*\}}{Pr\{|\eta^*| \geq 1\}}. \tag{3.26}$$

We now invoke Eq. (3.4) (compare Eqs. (3.20) and (3.3)) to bound the numerator of Eq. (3.26) by

$$K(R,P_1) \exp\{-nE(R,P_1)\} \tag{3.27}$$

where

$$P_b \equiv \frac{P_I}{N_e + P_J/b} \tag{3.28}$$

for all $b > 0$. From Lemma 2(b), we know that the denominator of Eq. (3.26) is not less than 1/4; therefore, combining Eqs. (3.26) and (3.24), we conclude that

$$\lambda^{PJ}(C_n^*) \leq 4K(R,P_1) \exp\{-nE(R,P_1)\} \tag{3.29}$$

for all $n \geq 1$. The right-hand side tends to zero as $n \to +\infty$, as desired. This completes the proof of the forward part of Theorem 1.

(b): $\mathbf{R}_{PI|PJ} \subset \hat{\mathbf{R}}_{PI|PJ}$.

Let $\epsilon > 0$, and suppose that $R \geq C_{PI\,|\,PJ} + \epsilon$. We claim that there exists a positive sequence $\{\gamma n\}_{n=1}^{\infty}$ such that

$$\lambda^{PJ}(C_n^*) \geq 1 - \gamma_n \tag{3.30}$$

is satisfied for all PI-admissible (n,M) random codes, C_n^*, where $R \equiv (1/n)\log_2 M$, and $\gamma_n \to 0$ as $n \to +\infty$. Clearly, (b) follows from Eq. (3.30).

To prove the claim, fix $\epsilon > 0$ and take $\delta > 0$ small enough so that

$$C_{PI\,|\,PJ} < \frac{1}{2}\log_2\left(1 + \frac{P_T}{N_e + P_J/(1+\delta)}\right) < C_{PI\,|\,PJ} + \epsilon \leq R\,, \tag{3.31}$$

and let $C_n^* = \{(\mathbf{u}_1^*, D_1^*), \ldots, (\mathbf{u}_M^*, D_M^*)\}$ be any (n, M) random code satisfying PI. If the jamming sequence $\mathbf{s}^*$ were i.i.d. $N(0, P_J/(1+\delta))$ random variables, then by Eq. (3.7) we know that

$$\begin{aligned}&\max_{1 \leq i \leq M} Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{P_J/(1+\delta)}\,\eta^* \in \bar{D}_i^*\} \\ &\quad \geq 1 - K'(R, P_{1+\delta}) \exp\{-nE'(R, P_{1+\delta})\}\end{aligned} \tag{3.32}$$

where $P_{(\cdot)}$ is as defined in Eq. (3.28). Unfortunately, $\sqrt{P_J/(1+\delta)}\,\eta^*$ does not satisfy PJ, therefore, we define a truncated noise process $\eta_i^*(\delta)$ as follows:

$$\eta_i^*(\delta) \equiv \begin{cases} \sqrt{P_J/(1+\delta)}\,\eta^*, & |\eta^*| \leq \sqrt{n(1+\delta)} \\ \dfrac{\sqrt{nP_J}}{|\eta^*|}\,\eta^*, & |\eta^*| \geq \sqrt{n(1+\delta)}\,, \end{cases} \tag{3.33}$$

so that $\eta_i^*(\delta)$ is clearly admissible under PJ. Now

$$\begin{aligned}&Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{P_J/(1+\delta)}\,\eta^* \in \bar{D}_i^*\} \\ &\quad = Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{PJ/(1+\delta)}\,\eta^* \,\big|\, |\eta^*| \leq \sqrt{n(1+\delta)}\} \times Pr\{|\eta^*| \leq \sqrt{n}(1+\delta)\} \\ &\quad + Pr\{\mathbf{u}_i^* + \eta_e^* + \sqrt{P_J/(1+\delta)}\,\eta^* \,\big|\, |\eta^*| > \sqrt{n(1+\delta)}\} \times Pr\{|\eta^*| > \sqrt{n}(1+\delta)\} \\ &\quad \leq Pr\{\mathbf{u}_i^* + \eta_e^* + \eta_i^*(\delta) \in \bar{D}_i^*\} + Pr\{|\eta^*| > \sqrt{n(1+\delta)}\}\,.\end{aligned} \tag{3.34}$$

From Lemma 2(a), the right-most expression in Eq. (3.34) is bounded above by $\exp\{-n\delta^2/12\}$ for all $n \geq n_0(\delta)$. Taking the maximum of Eq. (3.34) over all i and substituting Eq. (3.32), we conclude that

$$\begin{aligned}\lambda^{PJ}(C_n^*) &\geq \max_{1 \leq i \leq M} Pr\{\mathbf{u}_i^* + \eta_e^* + \eta_e^*(\delta) \in \bar{D}_i^*\} \\ &\geq 1 - K'(R, P_{1+\delta}) \exp\{-nE'(R, P_{1+\delta})\} - \exp\{-\frac{n}{12}\delta^2\}.\end{aligned} \tag{3.35}$$

for all $n \geq n_0(\delta)$ and all δ satisfying Eq. (3.31). The right-hand expression in Eq. (3.35) tends to unity as n increases *uniformly* over all codes of rate R, which is the desired result. This completes the proof of the strong converse to Theorem 1.

Proof of Theorem 2:

(a): $\hat{\mathbf{R}}_{PI\,|\,AJ} \supset \mathbf{R}_{PI\,|\,AJ}$

We retain the notation and results of part (a) of the proof of Theorem 1. Let R, nonnegative, be given, set $M_n \equiv \lfloor 2^{nR} \rfloor$, and let $\{C_n^*\}_{n=1}^{\infty}$ be the sequence of PI-admissible (n, M_n) random codes introduced in Eq. (3.19). We claim that there exists a positive sequence $\{\gamma_n\}_{n=1}^{\infty}$ so that

$$\lambda^{AJ}(C_n^*) \leqslant \lambda^{PI\,|\,AJ}(R) + \gamma_n, \tag{3.36}$$

and $\gamma_n \to 0$; this implies (a).

To prove Eq. (3.36), let $\mathbf{s}^*$ be any jamming sequence that satisfies AJ and let λ be such that $0 < \lambda \leqslant 1$. As demonstrated in part (a) of the proof of Theorem 1 (cf. Eq. (3.29)), if

$$R < \frac{1}{2}\log_2\left(1 + \frac{P_I}{N_e + P_J/\lambda}\right) = C_{PI\,|\,AJ}(\lambda), \tag{3.37}$$

then for each $1 \leqslant i \leqslant M_n$

$$Pr\left\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \mathbf{s}^* \in \bar{A}_1^* \,\middle|\, \frac{1}{n}\sum_{i=1}^{n} s_i^{*2} \leqslant P_J/\lambda\right\} \leqslant 4K(R, P_\lambda)\exp\{-nE(R, P_\lambda)\}, \tag{3.38}$$

where $P_{(\cdot)}$ is defined in Eq. (3.28). Since $\mathbf{s}^*$ satisfies AJ, Chebyshev's inequality (e.g. Ref. 13) yields

$$Pr\left\{\frac{1}{n}\sum_{i=1}^{n} s_i^{*2} > P_J/\lambda\right\} \leqslant \lambda. \tag{3.39}$$

Using Eqs. (3.38) and (3.39), we can bound above the error probability incurred by any $\mathbf{s}^*$ satisfying AJ in the following way: For any λ such that Eq. (3.37) holds, we have

$$\begin{aligned} &Pr\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \mathbf{s}^* \in \bar{A}_i^*\} \\ &\quad = Pr\left\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \mathbf{s}^* \in \bar{A}_i^* \,\middle|\, \frac{1}{n}\sum_{i=1}^{n} s_i^{*2} \leqslant P_J/\lambda\right\} Pr\left\{\frac{1}{n}\sum_{i=1}^{n} s_i^{*2} \leqslant P_J/\lambda\right\} \\ &\quad + Pr\left\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \mathbf{s}^* \in \bar{A}_i^* \,\middle|\, \frac{1}{n}\sum_{i=1}^{n} s_i^{*2} \leqslant P_J/\lambda\right\} Pr\left\{\frac{1}{n}\sum_{i=1}^{n} s_i^{*2} > P_J/\lambda\right\} \\ &\quad \leqslant \lambda + 4K(R, P_\lambda)\exp\{-nE(R, P_\lambda)\}. \end{aligned} \tag{3.40}$$

Let $\{\lambda_n\}_{n=1}^{\infty}$ be any positive sequence such that $\lambda_n > \lambda^{PI\,|\,AJ}(R)$ (so that Eq. (3.37) holds) and $\lambda_n \to \lambda^{PI\,|\,AJ}(R)$ slowly enough so that

$$K(R, P_{\lambda_n})\exp\{-nE(R, P_{\lambda_n})\} \to 0. \tag{3.41}$$

Clearly, such a sequence exists. Taking the supremum of Eq. (3.40) over all i and AJ-admissible $\mathbf{s}^*$ and substituting λ_n, we then conclude that

$$\lambda^{AJ}(C_n^*) \leqslant \lambda_n + 4K(R, P_{\lambda_n})\exp\{-nE(R, P_{\lambda_n})\}. \tag{3.42}$$

The right-hand side of Eq. (3.42) tends to $\lambda^{PI|AJ}(R)$ as n increases, proving Eq. (3.36) and (a). This concludes the proof of the forward part of Theorem 2.

(b): $\mathbf{R}_{PI|AJ} \subset \hat{\mathbf{R}}_{PI|AJ}$.

We now prove that there exists a positive sequence $\{\gamma_n\}_{n=1}^{\infty}$ so that $\gamma_n \to 0$ as $n \to \infty$ and

$$\lambda^{AJ}(C_n^*) \geqslant \lambda^{PI|AJ}(R) - \gamma_n \tag{3.43}$$

is satisfied for all PI-admissible (n,M) random codes, where $R \equiv (1/n)\log_2 M$; (b) follows from Eq. (3.43).

First, let λ be such that $0 < \lambda \leqslant 1$. Suppose that a "pulsed" jamming sequence, say $\mathbf{s}_\lambda^*$, is defined to be

$$\mathbf{s}_\lambda^* \equiv \sqrt{P_J/\lambda}\, Z_\lambda^*\, \boldsymbol{\eta}^* \tag{3.44}$$

where $\boldsymbol{\eta}^*$ is a n-vector of i.i.d. $N(0,1)$ random variables, and Z_λ^* is a Bernoulli random variable that is independent of $\boldsymbol{\eta}^*$ and distributed as follows:

$$Pr\{Z_\lambda^* = 1\} = 1 - Pr\{Z_\lambda^* = 0\} = \lambda. \tag{3.45}$$

It is easy to verify that $\mathbf{s}_\lambda^*$ satisfies AJ for all $0 < \lambda \leqslant 1$ and all $n \geqslant 1$.

Suppose now that λ is such that

$$R > \frac{1}{2}\log_2\left(1 + \frac{P_T}{N_e + P_J/\lambda}\right) = C_{PI|AJ}(\lambda), \tag{3.46}$$

then the error probability of C_n^* can be bounded below in the following way:

$$\begin{aligned}
\lambda^{AJ}(C_n^*) &\overset{(a)}{\geqslant} \max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \mathbf{s}_\lambda^* \in \bar{D}_i^*\} \\
&\overset{(b)}{\geqslant} \max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \mathbf{s}_\lambda^* \in \bar{D}_i^* \,\big|\, Z_\lambda^* = 1\}\, Pr\{Z_\lambda^* = 1\} \\
&\overset{(c)}{=} \lambda\left(\max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \boldsymbol{\eta}_e^* + \sqrt{P_J/\lambda}\,\boldsymbol{\eta}^* \in \bar{D}_i^*\}\right) \\
&\overset{(d)}{\geqslant} \lambda\left(1 - K'(R,P_\lambda)\exp\{-nE'(R,P_\lambda)\}\right),
\end{aligned} \tag{3.47}$$

where P_λ is defined in Eq. (3.28). These steps are justified in the following way: (a) is an immediate consequence of the definition of $\lambda^{AJ}(\cdot)$; (b) follows from the law of total probability; (c) follows from Eqs. (3.44) and (3.45); and (d) is a consequence of Eqs. (3.46) and (3.7).

Let $\{\lambda_n\}_{n=1}^{\infty}$ be any positive sequence such that $\lambda_n < \lambda^{PI|AJ}(R)$ (so that Eq. (3.46) is satisfied) and $\lambda_n \to \lambda^{PI|AJ}(R)$ slowly enough so that

$$K'(R,P_{\lambda_n})\exp\{-nE'(R,P_{\lambda_n})\} \to 0.$$

Substitution of λ_n into Eq. (3.47) yields

$$\lambda^{AJ}(C_n^*) \geqslant \lambda_n \left(1 - K_1(R, A_{\lambda_n}) \exp\{-nE_1(R, A_{\lambda_n})\}\right) \tag{3.48}$$
$$\equiv \lambda^{PI|AJ}(R) - \gamma_n,$$

where $\{\gamma_n\}_{n=1}^{\infty}$ has the desired properties. This completes the proof of the strong converse to Theorem 2.

Proof of Theorem 3:

(a): $\mathbf{R}_{AI|PJ} \supset \hat{\mathbf{R}}_{AI|PJ}$.

Let R, nonnegative, be given and set $M_n = \lfloor 2^{nR} \rfloor$. For any $0 \leqslant \lambda < 1$, define a sequence of (n, M_n) random codes, say $\{C_n^*(\lambda)\}_{n=1}^{\infty}$, in the following way:

$$C_n^*(\lambda) \equiv \{(\mathbf{u}_1^*(\lambda), A_1^*), \ldots, (\mathbf{u}_{M_n}^*(\lambda), A_{M_n}^*)\}, \tag{3.49}$$

where

$$\mathbf{u}_i^*(\lambda) \equiv \sqrt{P_T/(1-\lambda)}\, Z_{1-\lambda}^* \mathbf{v}_i^*, \tag{3.50}$$

$Z_{1-\lambda}^*$ is a Bernoulli random variable independent of $\mathbf{v}_i^*$ such that

$$Pr\{Z_{1-\lambda}^* = 1\} = 1 - Pr\{Z_{1-\lambda}^* = 0\} = 1 - \lambda, \tag{3.51}$$

and $\hat{C}_n^* = \{(\mathbf{v}_1^*, A_1^*), \ldots, (\mathbf{v}_M^*, A_{M_n}^*)\}$ is the standard (n, M_n) random code, as in Eq. (3.1). It is easy to verify that $C_n^*(\lambda)$ satisfies AI for all $0 \leqslant \lambda < 1$, and all n. We further claim that there exists positive sequences $\{\lambda_n\}_{n=1}^{\infty}$ and $\{\gamma_n\}_{n=1}^{\infty}$ such that

$$\lambda^{PJ}(C_n^*(\lambda_n)) \leqslant \lambda^{AI|PJ}(R) + \gamma_n \tag{3.52}$$

and $\gamma_n \to 0$; this implies (a).

The proof of this claim is in the spirit as the converse to Theorem 2, so we shall be brief. Let $\mathbf{s}^*$ be any PJ-admissible jamming signal, and suppose λ is such that

$$R < C_{AI|PJ}(\lambda). \tag{3.53}$$

We can then bound the error probability above as follows:

$$\begin{aligned}
&Pr\{\mathbf{u}_i^*(\lambda) + \eta_c^* + \mathbf{s}^* \in \bar{A}_i^*\} \\
&\quad = Pr\{\mathbf{u}_i^*(\lambda) + \eta_c^* + \mathbf{s}^* \in \bar{A}_i^* | Z_{1-\lambda}^* = 0\}\, Pr\{Z_{1-\lambda}^* = 0\} \\
&\quad + Pr\{\mathbf{u}_i^*(\lambda) + \eta_c^* + \mathbf{s}^* \in \bar{A}_i^* | Z_{1-\lambda}^* = 1\}\, Pr\{Z_{1-\lambda}^* = 1\} \\
&\quad \overset{(a)}{\leqslant} \lambda + Pr\{\sqrt{P_I/(1-\lambda)}\,\mathbf{v}_i^* + \eta_c^* + \mathbf{s}^* \in \bar{A}_i^*\} \\
&\quad \overset{(b)}{\leqslant} \lambda + 4K(R, P^{\lambda}) \exp\{-nE(R, P^{\lambda})\},
\end{aligned} \tag{3.54}$$

where

$$P^{\lambda} \equiv \frac{P_J/(1-\lambda)}{N_c + P_J}. \tag{3.55}$$

The justification of these steps is as follows: (a) results when Eq. (3.51) is substituted into the preceding equation, and the first conditional probability is bounded above by one; (b) follows from Eqs. (3.53) and (3.29) and the fact that $\mathbf{s}^*$ satisfies PJ.

Now let $\{\lambda_n\}_{n=1}^{\infty}$ be any positive sequence such that $\lambda_n < \lambda^{PJ|AJ}(R)$, $\lambda_n \to \lambda^{PJ|AJ}(R)$, and

$$K(R,P^{\lambda_n}) \exp\{-nE(R,P^{\lambda_n})\} \to 0.$$

Taking the supremum of Eq. (3.54) over all i and PJ-admissible $\mathbf{s}^*$ and substituting λ_n, we find that

$$\begin{aligned} \lambda^{PJ}(C_n^*(\lambda_n)) &\leqslant \lambda_n + 4K(R,P^{\lambda_n}) \exp\{-nE(R,P^{\lambda_n})\} \\ &\equiv \lambda^{AJ|PJ}(R) + \gamma_n, \end{aligned} \tag{3.56}$$

where $\{\gamma_n\}_{n=1}^{\infty}$ has the desired properties. This completes the proof of the forward part of Theorem 3.

(b): $\mathbf{R}_{AI|PJ} \subset \hat{\mathbf{R}}_{AI|PJ}$.

We now prove that a positive sequence $\{\gamma_n\}_{n=1}^{\infty}$ exists, which depends only on R, so that $\gamma_n \to 0$ and

$$\lambda^{PJ}(C_n^*) \geqslant \lambda^{AI|PJ}(R) - \gamma_n \tag{3.57}$$

is satisfied for all AI-admissible (n,M) random codes, where $R \equiv (1/n)\log_2 M$; this implies (b).

To prove this, let

$$C_n^* = \{(\mathbf{u}^*_1, D^*_1), \ldots, (\mathbf{u}^*_M, D^*_M)\}$$

be any AI-admissible (n,M) random code. Fix $\delta > 0$, and let $\eta^*_t(\delta)$ be the PJ-admissible jamming sequence introduced in Eq. (3.33). As in part (b) of the proof of Theorem 2, it is easy to show that

$$\begin{aligned} \lambda^{PJ}(C_n^*) &\geqslant \max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \eta_c^* + \eta^*_t(\delta) \in \bar{D}_i\} \\ &\geqslant \max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \eta_c^* + \sqrt{P_J/(1+\delta)}\,\eta^* \in \bar{D}_i\} - \exp\left\{-\frac{n}{12}\delta^2\right\}. \end{aligned} \tag{3.58}$$

We now use Lemma 3 to lower bound the first expression on the right-hand side of Eq. (3.58):

$$\begin{aligned} &\max_{1 \leqslant i \leqslant M} Pr\left\{\mathbf{u}_i^* + \eta_c^* + \sqrt{P_J/(1+\delta)}\,\eta^* \in \bar{D}_i\right\} \\ &\quad \geqslant \frac{1}{M}\sum_{i=1}^{M} Pr\{\mathbf{u}_i^* + \eta_c^* + \sqrt{P_J/(1+\delta)}\,\eta^* \in \bar{D}_i^*\} \\ &\quad \geqslant Pr\{P(U^*(C_n^*)) < (4^{R-2\epsilon}-1)(N_c + P_J/(1+\delta))\} - \gamma_n(\epsilon), \end{aligned} \tag{3.59}$$

where $U^*(\cdot)$ is defined just prior to Lemma 3, and $\gamma_n(\epsilon)$ is as defined in Eq. (3.11). Recall the definition of $\lambda^{AI|PJ}(R)$ in Eq. (2.19); when we want to exhibit the dependence of this function on P_J, we use the notation $\lambda^{AI|PJ}(R;P_J)$. Since C_n^* satisfies AI, it is true that $\mathbf{E}P(U(C_n^*)) \leqslant P_I$. Using this and Chebysheff's inequality, we can easily show that

$$Pr\{ P(U^*(C_n^*)) < (4^{R-2\epsilon}-1)(N_e + P_J/(1+\delta)) \} \geqslant \lambda^{AI|PJ}(R-2\epsilon; P_J/(1+\delta)). \tag{3.60}$$

Therefore, combining Eqs. (3.58), (3.59), and (3.60), we conclude that for all $\epsilon > 0$ and $\delta > 0$,

$$\lambda^{PJ}(C_n^*) \geqslant \lambda^{AI|PJ}(R-2\epsilon; P_J/(1+\delta)) - \exp\left\{-\frac{n}{12}\delta^2\right\} - \gamma_n(\epsilon). \tag{3.61}$$

Note that the right-hand of Eq. (3.61) depends on C_n^* only through the rate R. Now choose $\{\delta_n\}_{n=1}^{\infty}$, both depending only on R and decreasing to zero slowly enough so that the last two terms in the right-hand of Eq. (3.61) converge to zero. The right-hand expression then tends to $\lambda^{AI|PJ}(R)$, as desired. This completes the proof of the strong converse to Theorem 3.

Proof of Theorem 4:

(a): $\mathbf{R}_{AI|AJ} \supset \hat{\mathbf{R}}_{AI|AJ}$.

For any nonnegative R, set $M_n \equiv \lfloor 2^{nR} \rfloor$. Fix $\epsilon > 0$ and define a sequence of AI-admissible (n, M_n) random codes, say

$$C_n^*(\epsilon) \equiv \{ (\mathbf{u}_1^*(\epsilon), A_1^*), \ldots, (\mathbf{u}_{M_n}^*(\epsilon), A_{M_n}^*) \}, \tag{3.62}$$

where

$$\mathbf{u}_i^*(\epsilon) \equiv \sqrt{P_0^*(\epsilon)}\,\mathbf{v}_i^*; \tag{3.63}$$

$P_o^*(\epsilon)$ is a nonnegative random variable, independent of $\mathbf{v}^*$ that satisfies $\mathbf{E}\,P_0^*(\epsilon) \leqslant P_T$, and whose distribution will be given below; and $\hat{C}_n^* = \{(\mathbf{v}_i^*, A_i^*)\}_{i=1}^{M_n}$ is the standard (n, M_n) random code. It is easy to verify that $C_n^*(\epsilon)$ satisfies AI for all $0 \leqslant \lambda < 1$, and all n. We claim that there are positive sequences $\{\epsilon_n\}_{n=1}^{\infty}$ and $\{\gamma_n\}_{n=1}^{\infty}$ such that

$$\lambda^{AJ}(C_n^*(\epsilon_n)) \leqslant \lambda^{AI|AJ}(R) + \gamma_n, \tag{3.64}$$

and $\gamma_n \to 0$; this implies (a).

In proving this claim, we assume that $N_e > 0$; the proof if $N_e = 0$ is similar. We refer the reader to the Theorem of Appendix C, and adopt the notation used there. A consequence of this theorem (cf. Eq. (C4)) is that if X_0 has the distribution Eq. (C28b) and v_0 is as defined in Eq. (C28a), then

$$Pr\{ X_0 \geqslant Y + c \} \geqslant v_0 \tag{3.65}$$

holds for all nonnegative random variables Y that satisfy $\mathbf{E}\,Y \leqslant b$.

Now make the following substitutions:

$$a = \frac{P_I}{(4^{R+\epsilon}-1)}, \; b = P_J, \; c = N_e,$$

and define $P_o^*(\epsilon)$ in Eq. (3.63) by

$$P_o^*(\epsilon) \equiv (4^{R+\epsilon} - 1) X_0.$$

With these substitutions, it is easy to verify that

$$v_0 = 1 - \lambda^{AI|AJ}(R + \epsilon).$$

> From Eq. (3.65), it follows that if J^* is any nonnegative random variable that satisfies $\mathbf{E}J^* \leqslant P_J$, then

$$Pr\{ P_o^*(\epsilon) < (4^{R+\epsilon} - 1)(N_e + J^*) \} \leqslant \lambda^{AI|AJ}(R + \epsilon). \tag{3.66}$$

Let $\mathbf{s}^*$ be any AJ-admissible jamming sequence and define $J^* = |\mathbf{s}^*|^2$ (so that $\mathbf{E}J^* \leqslant = P_J$), and set $\hat{\mathbf{s}}^* \equiv \mathbf{s}^*/\sqrt{J^*}$ when $J^* > 0$ and $\hat{\mathbf{s}}^* \equiv 0$ otherwise (so that $|\hat{\mathbf{s}}^*| \leqslant 1$ a.s.). In the proof of Theorem 1 (cf. Eq. (3.29)) we showed that if $|\hat{\mathbf{s}}^*| \leqslant 1$ a.s. and P and J are positive constants, then

$$Pr\{ \sqrt{P_o^*(\epsilon)}\, \mathbf{v}_i^* + \boldsymbol{\eta}_e^* + \sqrt{J^*}\, \hat{\mathbf{s}}^* \in \bar{A}_i^* \mid P_o^*(\epsilon) = P, J^* = J \}$$

$$\leqslant 4K(R, P') \exp\{ -nE(R, P') \}, \tag{3.67}$$

for all $n \geqslant 1$, provided that

$$P' \equiv \frac{P}{N_e + J} > (4^R - 1).$$

In particular, if

$$\frac{P}{N_e + J} > (4^{R+\epsilon} - 1), \tag{3.68}$$

then using Eq. (3.5b) we can further upper bound the right-hand side of Eq. (3.67) by

$$\bar{B}_n(R, \epsilon) \equiv 4K(R, 4^{R+\epsilon} - 1) \exp\{ - nE(R, 4^{R+\epsilon} - 1) \}. \tag{3.69}$$

Note that $\bar{B}_n(R, \epsilon) \to 0$ for all $\epsilon > 0$. Now define

$$h_n(P, J) \equiv \begin{cases} \bar{B}_n(R, \epsilon) & P > (4^{R+\epsilon} - 1)(N_e + J) \\ 1 & \text{otherwise} \end{cases} \tag{3.70}$$

so that $h_n(P, J)$ is an upper bound on Eq. (3.67) *for all* P, J, and n. Averaging this bound over the distributions of $C_n^*(\epsilon)$ and J^*, we find that

$$\begin{aligned} Pr\{ \mathbf{u}_i^*(\epsilon) + \boldsymbol{\eta}_e^* + \mathbf{s}^* \in \bar{A}_i^* \} &= Pr\{ \sqrt{P_0^*(\epsilon)}\, \mathbf{v}_i^* + \boldsymbol{\eta}_e^* + \sqrt{J^*}\, \hat{\mathbf{s}}^* \in \bar{A}_i^* \} \\ &\leqslant \mathbf{E}\, h_n(P_0^*(\epsilon), J^*) \\ &= \bar{B}_n(R, \epsilon) + (1 - \bar{B}_n(R, \epsilon))\, Pr\{ P_0^*(\epsilon) \leqslant (4^{R+\epsilon} - 1)(N_e + J^*) \} \\ &\leqslant \bar{B}_n(R, \epsilon) + \lambda^{AI|AJ}(R + \epsilon), \end{aligned} \tag{3.71}$$

where the last inequality follows from Eq. (3.66). Taking the supremum of Eq. (3.71) over all i and AJ-admissible $\mathbf{s}^*$, we obtain the bound

$$\lambda^{AJ}(C_n^*(\epsilon)) \leqslant \bar{B}_n(R,\epsilon) + \lambda^{AI|AJ}(R+\epsilon), \tag{3.72}$$

for all $\epsilon > 0$, $n \geqslant 1$. The claim Eq. (3.64) now follows by choosing $\{\epsilon_n\}_{n=1}^{\infty}$ to decrease to zero slowly enough so that $\bar{B}_n(R,\epsilon_n) \to 0$; since $\lambda^{AI|AJ}(\cdot)$ is continuous, the right-hand term then tends to $\lambda^{AI|AJ}(R)$, as desired. This completes the proof of the forward part of Theorem 4.

(b): $\mathbf{R}_{AI|AJ} \subset \hat{\mathbf{R}}_{AI|AJ}$.

We now prove that there is a positive sequence $\{\gamma_n\}_{n=1}^{\infty}$ that depends only on R, so that $\gamma_n \to 0$ and

$$\lambda^{AJ}(C_n^*) \geqslant \lambda^{AI|AJ}(R) - \gamma_n \tag{3.73}$$

is satisfied for any AI-admissible (n, M) random code C_n^*, where $R \equiv (1/n)\log_2 M$; this implies (b).

Fix $\epsilon > 0$. As in part (a) of the proof of Theorem 4, we invoke the Theorem of Appendix C. This Theorem implies that if Y_0 has the distribution Eq. (C28c), and v_0 is as defined in Eq. (C28a), then

$$Pr\{X \geqslant Y_0 + c\} \leqslant v_0 \tag{3.74}$$

holds for all nonnegative random variables X that satisfy $\mathbf{E}X \leqslant a$. Making the substitution

$$a = \frac{P_T}{(4^{R-2\epsilon}-1)}, \; b = P_J, \; c = N_c,$$

and defining

$$J_0^*(\epsilon) \equiv Y_0,$$
$$P^* \equiv (4^{R-2\epsilon}-1)X,$$

we obtain that

$$v_0 = 1 - \lambda^{AI|AJ}(R-2\epsilon)$$

and

$$Pr\{P^* < (4^{R-2\epsilon}-1)(N_c + J_0^*(\epsilon))\} \geqslant \lambda^{AJ|AJ}(R-2\epsilon) \tag{3.75}$$

holds for all P^* satisfying

$$EP^* \leqslant P_I. \tag{3.76}$$

Note that $\sqrt{J_0^*(\epsilon)}\eta^*$ is AI-admissible for all $\epsilon > 0$.

Let C_n^* be any (n, M) random code. We may bound the error probability of this code below as follows:

$$\begin{aligned}\lambda^{AJ}(C_n^*) &\geqslant \max_{1 \leqslant i \leqslant M} Pr\{\mathbf{u}_i^* + \eta_\epsilon^* + \sqrt{J_0^*(\epsilon)}\eta^* \in \bar{D}_i^*\} \\ &\geqslant \frac{1}{M}\sum_{i=1}^{M} Pr\{\mathbf{u}_i^* + \eta_\epsilon^* + \sqrt{J_0^*(\epsilon)}\eta^* \in \bar{D}_i^*\} \\ &\overset{(a)}{\geqslant} Pr\{P(U^*(C_n^*)) < (4^{R-2\epsilon}-1)(N_\epsilon + J_0^*(\epsilon))\} - \gamma_n(\epsilon) \\ &\overset{(b)}{\geqslant} \lambda^{AI|AJ}(R-2\epsilon) - \gamma_n(\epsilon), \end{aligned} \tag{3.77}$$

where $\gamma_n(\epsilon)$ is defined in Eq. (3.11). The justification of these steps is as follows: (a) results by applying Lemma 3; (b) follows from Eq. (3.75) and the fact that $\mathbf{E}P(U^*(C_n^*)) \leqslant P_T$. Now choose a decreasing sequence of positive numbers, $\{\epsilon_n\}_{n=1}^{\infty}$, such that $\epsilon_n \to 0$ slowly enough so that $\gamma_n(\epsilon_n) \to 0$. Substituting ϵ_n into the right-hand side of Eq. (3.77), we obtain an expression that tends to $\lambda^{AI|AJ}(R)$ uniformly for all AI-admissible codes of rate R, as desired. This completes the proof of the strong converse to Theorem 4.

4. DISCUSSION

Our results show that the asymptotic behavior of GAVCs is qualitatively different from that of discrete AVC: whereas the latter always have a random coding capacity (cf. Blackwell *et al.* [1]), the former generally have no capacity (except in the case PI | PJ). This is a direct consequence of the imposition of power constraints of the *average* type.

It remains to determine, if they exist, the corresponding λ-capacities for the GAVC when the transmitter is restricted to *deterministic* codes (i.e., those of the form Eq. (2.2)). For the discrete AVC, deterministic coding capacities are known in many special cases. Ahlswede [14], using the average probability of error concept, has shown that the capacity of the discrete AVC is either equal to the random coding capacity, or else it is zero.† This method apparently fails for the GAVC, owing to the presence of a cost structure on the allowable channels and encoders.

The coding problems of Section 2 lend themselves to an alternative game theoretic formulation. Corresponding to each GAVC, say A | B, there is a family of two-player, zero-sum games (cf. Blackwell and Girshik [15]) defined as follows. Fix the blocklength n and the source rate R. The transmitter's (resp. jammer's) *allowable strategies* consist of all $(n, 2^{nR})$ random codes, C_n^* (resp. all $\mathbf{R}^n$ -valued random vectors, $\mathbf{s}^*$) that satisfy the power constraint A (resp. B). The payoff when the jammer plays $\mathbf{s}^*$ and the transmitter plays C_n^* is the error probability $\lambda(C_n^*, \mathbf{s}^*)$, defined in Eq. (2.8). The jammer wants to maximize this probability; the transmitter wants to minimize it. Therefore, they seek strategies that attain the outer extrema in the following programs:

$$\textit{Transmitter's Program}: \bar{\nu}_n \equiv \inf_{C_n^*} \sup_{\mathbf{s}^*} \lambda(C_n^*, \mathbf{s}^*), \tag{4.1a}$$

$$\textit{Jammer's Program}: \underline{\nu}_n \equiv \sup_{\mathbf{s}^*} \inf_{C_n^*} \lambda(C_n^*, \mathbf{s}^*), \tag{4.1b}$$

where the extrema are taken over all allowable $\mathbf{s}^*$ and C_n^*. An *optimal strategy* for the transmitter (resp. jammer), if it exists, is one that attains the outer extrema in the transmitter's (resp. jammer's) program. For any $\epsilon > 0$, *ϵ-optimal strategies*, $C_{n\epsilon}^*$ and $\mathbf{s}_\epsilon^*$, are allowable strategies for which

$$\sup_{\mathbf{s}^*} \lambda(C_{n\epsilon}^*, \mathbf{s}^*) \leqslant \bar{\nu}_n + \epsilon, \tag{4.2}$$

$$\inf_{C_n^*} \lambda(C_n^*, \mathbf{s}_\epsilon^*) \geqslant \underline{\nu}_n - \epsilon, \tag{4.3}$$

†At present, no simple, general method is known for deciding between these two alternatives

where the extrema are taken over all allowable $\mathbf{s}^*$ and C_n^*. It is always true that $\underline{\nu}_n \leqslant \bar{\nu}_n$; if $\underline{\nu}_n = \nu_n$, then the game is said to have a *value*: $\nu_{on} \equiv \underline{\nu}_n = \bar{\nu}_n$.

Equation (4.1a) defines a sequence (in n) of communications games. Basar and Wu [6] have considered games of this type for a memoryless Gaussian source and for a different cost function, viz., mean-square distortion. For each n, they obtain the value of the game and characterize saddle-point strategies for each player. In contrast, we can say little about each game in the sequence; we can, however, say a great deal about the *asymptotic behavior* of the sequence.

Implicit in the proofs of Theorems 1 to 4 is the following result: The sequences $\{\underline{\nu}_n\}_{n=1}^{\infty}$ and $\{\bar{\nu}n\}_{n=1}^{\infty}$ converge, and

$$\lim_{n \to +\infty} \underline{\nu}_n = \lim_{n \to +\infty} \bar{\nu}_n = \lambda^{A|B}(R) \tag{4.4}$$

holds for every R and every pair of constraints A | B. Thus the sequence of games has an "asymptotic value" equal to $\lambda^{A|B}(R)$. Furthermore, for all $\epsilon > 0$, there exists, for all sufficiently large n, ϵ-optimal strategies for both transmitter and jammer. (Such strategies for the transmitter are explicitly constructed in the forward parts of the proofs in Section 3; jamming strategies are constructed in the converse parts.)

Some authors further constrain the jammer to signals of the form

$$\mathbf{s}^* = (z_1^* \eta_1^*, \ldots, z_n^* \eta_n^*), \tag{4.5}$$

where $\{\eta_i^*\}_{i=1}^n$ is i.i.d. $N(0,1)$ and $\{z_i^*\}_{i=1}^n$ is a sequence of random variables independent of $\{\eta_i^*\}_{i=1}^n$ and subject only to the average power constraint

$$\mathbf{E}\left\{\frac{1}{n}\sum_{i=1}^{n} z_i^{*2}\right\} \leqslant P_J.$$

We call this constraint AJG, and use the notation GAVC A | AJG to refer to the channel with input constraint A and jamming power constraint AJG. Since AJG is more restrictive than AJ, we must have $\mathbf{R}_{A|AJG} \supset \mathbf{R}_{A|AJ}$. However, the jamming strategies constructed in the converses to Theorems 2 and 4 are all of the form Eq. (4.5), so that we must have $\mathbf{R}_{A|AJG} = \mathbf{R}_{A|AJ}$ and consequently

$$\lambda^{A|AJG}(R) = \lambda^{A|AJ}(R). \tag{4.6}$$

Thus our results extend to Gaussian jammers.

It is especially interesting that the achievable regions of Theorems 2 to 4 are not determined solely by a simple optimization program involving mutual information, as is usually the case in information theory. McEliece and Stark [8] have modeled the conflict between transmitter and jammer, when coding is used, by a two-player, zero-sum game with *mutual information* as the payoff function. As an example, they considered the channel that we have called the GAVC AI | AJ (for the special case $N_e = 0$) and obtained the following results: Optimal transmission strategies for both players are i.i.d Gaussian sequences of maximum power and of length n, and the value (or optimal payoff) is

$$\frac{n}{2}\log_2\left(1 + \frac{P_T}{P_J}\right).$$

If the value of the game considered by McEliece-Stark is actually the capacity of the channel (the authors do not assert that it is), then it carries the following interpretation: when n is large and

$$R < \frac{1}{2}\log_2\left(1 + \frac{P_T}{P_J}\right),$$

then $\lambda^{AJ}(C_n^*) \approx 0$ is possible. In contrast, however, note that the ϵ-optimal strategies for the game AI | AJ in Eq. (4.1a) (cf. proof of Theorem 4) are *not* memoryless, and the error probability of any positive rate code is bounded away from zero. It is of considerable interest that these two apparently related games lead to such different results.

An explanation of this disparity between predictions of these two games lies in the fact that mutual information takes on operational significance only when the block length is large compared to the memory of the channel. The error probability formulation (i.e., Eq. (4.1a)) allows the jamming memory to equal the blocklength, whereas the mutual information formulation always assumes that the blocklength of the code is large compared to the jamming memory. Therefore the game involving mutual information gives an *a priori* advantage to the transmitter, and it is not surprising that this approach leads to much more optimistic results for the transmitter. We conclude that, at least for GAVCs, one must be careful in attributing a coding significance to games having mutual information as a payoff function.

From a practical viewpoint, the results of this report may be difficult to achieve or may lack meaning for a real jammer. Like the pulse-jamming signals considered by Houston [16], our ϵ-optimal strategies demand high peak power when R is small; unlike Houston's, however, this peak power must be sustained over the blocklength of the code. When n is large, the average power constraints (AI, AJ) may fail to reflect all the physical constraints that would limit a practical system. An extreme example: let $n \to +\infty$, then the optimal jamming strategy for the case PI | AJ is of the form: $s_i^* \sim N(0, P_J/\rho)$ *for all time* with probability ρ, and $s_i = 0$ *for all time* with probability $1 - \rho$. One may approach a more realistic situation by considering multiple constraints on the jammer (as discussed in Section 2).

5. ACKNOWLEDGMENTS

The authors thank Anthony Ephremides for many helpful discussions of this problem. This work was carried out while the first author was a Fellow at the Information Technology Division of the Naval Research Laboratory. It is a pleasure to acknowledge the excellent working conditions there, and to thank Dennis McGregor and Jeffrey Wieselthier of the Naval Research Laboratory for many stimulating discussions.

6. REFERENCES

1. D. Blackwell, L. Breiman, and A.J. Thomasian, "The Capacities of Certain Channel Classes Under Random Coding," *Ann. Math. Stat.* **31**, 558-567 (1960).

2. J. Wolfowitz, *Coding Theorems of Information Theory* (Springer-Verlag, Berlin, 1978), 3rd ed.

3. I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems* (Academic Press, New York, 1981).

4. N.M. Blachman, "On the Capacity of a Band-Limited Channel Perturbed by Statistically Dependent Interference," *IRE Trans. Inform. Theory* **IT-8**, 48-55, Jan. 1962.

5. N.M. Blachman, "The Effect of Statistically Dependent Interference upon Channel Capacity," *IRE Trans. Inform. Theory* **IT-8**, 553-557, Sept. 1962.

6. T. Basar and Y.-W. Wu, "Solutions to a Class of Minimax Decision Problems Arising in Communications Systems," *preprint*, 1984.

7. R.L. Dobrushin, "Optimal Information Transmission over a Channel with Unknown Parameters," *Radiotekh. Eletron.* **4** (12), 1951-1956 (1959).

8. R.J. McEliece and W.E. Stark, "An Information-Theoretic Study of Communication in the Presence of Jamming," *Proc. IEEE International Conference on Communications*, pp. 45.3.1-45.3.5 (1981).

9. M.K. Simon, J.K. Omura, R.A. Scholtz, and B.K. Levitt, *Spread-Spectrum Communication* (Computer Science Press, Rockville, Maryland, 1985), Vol. 1.

10. C.E. Shannon, "Probability of Error for Optimal Codes in a Gaussian Channel," *Bell Syst. Tech. J.* **38** (3), 611-656, May 1959.

11. R.G. Gallager, "A Simple Derivation of the Coding Theorem and Some Applications," *IEEE Trans. Inform. Theory* **IT-11**, 3-18, Jan. 1965.

12. S. Arimoto, "On the Converse to the Coding Theorem for Discrete Memoryless Channels," *IEEE Trans. Inform. Theory* **IT-19** (3), 357-359, May 1973.

13. P. Billingsley, *Probability and Measure* (Wiley, New York, 1979).

14. R. Ahlswede, "Elimination of Correlation in Random Codes for Arbitrarily Varying Channels," *Z. Wahrscheinlichkeitstheorie Verw. Gebiete* **44**, 159-175 (1978).

15. D. Blackwell and M.A. Girshick, *Theory of Games and Statistical Decisions* (Wiley, New York, 1954) (reprinted by Dover 1979).

16. 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 Aeronautics and Electronics Conference (NAECON)*, 51-58 (1975).

Appendix A

Proof of Lemma 1: To prove Lemma 1(a), let $\mathbf{s}$ and ω^* be as in the statement of the lemma, let ω be any unit vector in $\mathbf{R}^n$, and let T be any orthogonal transformation on $\mathbf{R}^n$ that maps $\mathbf{s}$ into $|\mathbf{s}|\omega$, i.e., so that

$$T\mathbf{s} = |\mathbf{s}|\omega .$$

Since minimum distance decoding is used (and distances are preserved by T), the following holds almost surely:

$$Pr\{ \mathbf{v}_l^* + \eta_c^* + \mathbf{s} \in \bar{A}_l^* \} = Pr\{ T\mathbf{v}_l^* + T\eta_c^* + |\mathbf{s}|\omega \in T\bar{A}_l^* \} .$$

The sets $\{ T\bar{A}_l^* \}_{l=1}^{M}$ remain minimum distance decoding sets for the codewords $\{ T\mathbf{v}_l^* \}_{l=1}^{M}$ and η_c^* are spherically symmetric, and so are unchanged by T. We conclude that

$$Pr\{ \mathbf{v}_l^* + \eta_c^* \, \mathbf{s} \in \bar{A}_l^* \} = Pr\{ \mathbf{v}_l^* + \eta_c^* + |\mathbf{s}|\omega \in \bar{A}_l^* \} ,$$

for all ω in the ensemble of ω^*, from which Lemma 1(a) immediately follows.

We now prove (b). Let the random variable m_l^* be defined by

$$m_l^* \equiv | \eta_c^* + l\omega^* |$$

and let $F_l(m)$ be its distribution function. It is easy to verify that, conditioned on the occurrence $m_l^* = m$, the expression $\eta_c^* + l\omega^*$ is uniformly distributed on the n-sphere of radius m; hence, its conditional distribution does not depend on l. Therefore, define the quantity

$$\gamma(m) \equiv Pr\{ \mathbf{u}_l^* + \eta_c^* + l\omega \in \bar{A}_l^* \, | \, | \eta_c^* + l\omega^* | = m \} . \tag{A1}$$

Since A^*_1 is a set formed by the minimum distance rule, if $m < \hat{m}$ then

$$\mathbf{u}_l^* + m \left(\frac{\eta_c^* + l\omega^*}{m_l^*} \right) \in \bar{A}_l^*$$

implies

$$\mathbf{u}_l^* + \hat{m} \left(\frac{\eta_c^* + l\omega^*}{m_l^*} \right) \in \bar{A}_l^*$$

and consequently, $\gamma(\cdot)$ is monotone increasing. If for each m, $F_1(m)$ is monotone decreasing as a function of l, then

$$\int_0^\infty \gamma(m) \, dF_j(m) \leqslant \int_0^\infty \gamma(m) \, dF_l(m) ,$$

which, according to Eq. (A1), is simply Lemma 1(b) disguised in different notation. It therefore only remains to show that

$$Pr\{ | \eta_c^* + l\omega^* | \leqslant m \} \leqslant Pr\{ | \eta_c^* + \hat{l}\omega^* | \leqslant m \} . \tag{A2}$$

We shall, in fact, prove a stronger result that implies Eq. (A2):

$$Pr\{ | \eta_c^* + l\omega^* |^2 \leqslant m^2 \mid \omega^* = \omega \} \leqslant Pr\{ | \eta_c^* + \hat{l}\omega^* |^2 \leqslant m^2 \mid \omega^* = \omega \}$$

for all ω. The latter inequality is an immediate consequence of the fact that the distribution of η_c^* decreases monotonically and symmetrically with distance from the origin. This completes the proof of part (b), and Lemma 1.

Appendix B

Proof of Lemma 2: Let $\{\eta_i^*\}_{i=1}^{\infty}$ be an i.i.d $N(0,1)$ sequence. To prove Lemma 2(a), note that 2(a) is trivially true when $\epsilon > 0$; therefore take $\epsilon > 0$. We apply Chernoff's bounding technique (e.g. Wozencraft and Jacobs [B1], Section 2.5) to obtain the following bounds:

$$Pr\left\{ \frac{1}{n} \sum_{i=1}^{n} \eta_i^2 \geq 1 + \epsilon \right\} \leq [\sqrt{1+\epsilon}\, e^{-\epsilon/2}]^n \tag{B1}$$

$$= \exp\left\{ \frac{n}{2} (\ln(1+\epsilon) - \epsilon) \right\}$$

$$Pr\left\{ \frac{1}{n} \sum_{i=1}^{n} \eta_i^{*2} \leq 1-\epsilon \right\} \leq [\sqrt{1-\epsilon}\, e^{\epsilon/2}]^n \tag{B2}$$

$$= \exp\left\{ \frac{n}{2} (\ln(1-\epsilon) + \epsilon) \right\}.$$

We now make use of a well-known (e.g. Olmstead [B2]) expansion for $\ln(1+x)$:

$$\ln(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} + \int_0^z \frac{(-t)^3}{1+t}\, dt, \quad -1 < x \leq 1. \tag{B3}$$

Let us use Eq. (B3) to derive approximations to the expressions that appear in the exponents of Eqs. (B1) and (B2); viz.,

$$\ln(1+\epsilon) - \epsilon = -\frac{\epsilon^2}{2} + \frac{\epsilon^3}{3} - \int_0^{\epsilon} \frac{t^3}{1+t}\, dt \tag{B4}$$

$$\leq -\frac{\epsilon^2}{2} + \frac{\epsilon^3}{3} = -\frac{\epsilon^2}{2}\left[1 - \frac{2\epsilon}{3}\right]$$

$$\ln(1-\epsilon) + \epsilon = -\frac{\epsilon^2}{2} - \frac{\epsilon^3}{3} - \int_0^{\epsilon} \frac{t^3}{1-t}\, dt \tag{B5}$$

$$\leq -\frac{\epsilon^2}{2} - \frac{\epsilon^3}{3} \leq -\frac{\epsilon^2}{2}\left[1 - \frac{2\epsilon}{3}\right].$$

Substituting these approximations into Eqs. (B1) and (B2), we obtain

$$Pr\left\{ \left| \frac{1}{n} \sum_{i=1}^{n} \eta_i^{*2} - 1 \right| \leq \epsilon \right\} \tag{B6}$$

$$= Pr\left\{ \frac{1}{n} \sum_{i=1}^{n} \eta_i^{*2} \geq 1 + \epsilon \right\} + Pr\left\{ \frac{1}{n} \sum_{i=1}^{n} \eta_i^{*2} \leq 1 - \epsilon \right\}$$

$$\leq 2 \exp\left\{ -\frac{n\epsilon^2}{4}\left[1 - \frac{2\epsilon}{3}\right] \right\} \leq \exp\left\{ -\frac{n\epsilon^2}{12} \right\}.$$

The last inequality holds for all n larger than $n_0(\epsilon) = 6 \ln 2/\epsilon^2(1-\epsilon)$, which depends only on ϵ. This completes the proof of Lemma 2(a).

We now prove Lemma 2(b). For $n = 1$ and 2, by direct calculation we obtain

$$Pr\{\eta_1^{*2} \geq 1\} = 0.3174, \tag{B7}$$

and

$$Pr\left\{\frac{1}{2}\sum_{i=1}^{2}\eta_i^{*2} \geq 1\right\} = e^{-1} = 0.3679, \tag{B8}$$

so that Lemma 2(b) holds for these values of n. For $n \geq 3$, we proceed as follows:

$$\begin{aligned} Pr\left\{\frac{1}{n}\sum_{i=1}^{n}\eta_i^{*2} \geq 1\right\} &\overset{(a)}{=} \int_n^\infty \frac{\alpha^{(n-2)/2}e^{-\alpha/2}}{2^{n/2}\Gamma\left(\frac{n}{2}\right)}\,d\alpha \\ &\overset{(b)}{=} \frac{n^{(n-2)/2}e^{-n/2}}{2^{(n-2)/2}\Gamma\left(\frac{n}{2}\right)} + \int_{n-2}^\infty \frac{\alpha^{(n-4)/2}e^{-\alpha/2}}{2^{(n-2)/2}\Gamma\left(\frac{n-2}{2}\right)}\,d\alpha \\ &\overset{(c)}{=} Pr\left\{\frac{1}{n-2}\sum_{i=1}^{n-2}\eta_i^{*2} \geq 1\right\} + \epsilon_n, \end{aligned} \tag{B9}$$

where

$$\epsilon_n \equiv \frac{n^{(n-2)/2}e^{-n/2}}{2^{(n-2)/2}\Gamma\left(\frac{n}{2}\right)} - \int_{n-2}^{n} \frac{\alpha^{(n-4)/2}e^{-\alpha/2}}{2^{(n-2)/2}\Gamma\left(\frac{n-2}{2}\right)}\,d\alpha. \tag{B10}$$

These steps are justified in the following way: (a) follows from the observation that $\sum_{i=1}^{n}\eta_i^{*2}$ has the standard chi-square density with n degrees of freedom (cf. [B3]); (b) follows from (a) by using integration by parts; and (c) is merely a rearrangement of (b).

We now claim that $\epsilon_n > 0$ for all $n \geq 3$. If true, this together with Eq. (B9), (B7), and (B8) would imply (b). To prove this claim, bound the integral in Eq. (B10) as follows:

$$\begin{aligned} \int_{n-2}^{n} \frac{\alpha^{(n-4)/2}e^{-\alpha/2}}{2^{(n-2)/2}\Gamma\left(\frac{n-2}{2}\right)}\,d\alpha &\overset{(a)}{=} \frac{n^{n/2}e^{-n/2}}{2^{(n-2)/2}\Gamma\left(\frac{n-2}{2}\right)} \int_{n-2}^{n} \left[\left(\frac{\alpha}{n}\right)e^{(1-\alpha/n)}\right]^{n/2}\frac{d\alpha}{\alpha^2} \\ &\overset{(b)}{<} \frac{n^{n/2}e^{-n/2}}{2^{(n-2)/2}\Gamma\left(\frac{n-2}{2}\right)} \int_{n-2}^{n}\frac{d\alpha}{\alpha^2} \\ &\overset{(c)}{=} \frac{n^{(n-2)/2}e^{-n/2}}{2^{(n-2)/2}\Gamma\left(\frac{n}{2}\right)}. \end{aligned}$$

Equation (a) is simply a rearrangement of factors; (b) follows by observing that the bracketed expression is strictly less than one when $\alpha/n < 1$; (c) results when the integral in (b) is evaluated. This completes the proof of the claim and Lemma 2.

Appendix C

In this appendix, we study the following two-player, zero-sum game (cf. Blackwell and Girshik [C1]). Let a, b, and c be real numbers such that $a, b > 0$ and $c \geq 0$. Player I's (respectively, player II's) allowable *strategies* consist of all nonnegative, real-valued, random variables X (resp. Y) satisfying $EX \leq a$ (resp. $EY \leq b$).* The payoff to player I, when I plays X and II plays Y, is

$$Pr\{X \geq Y + c\}. \tag{C1}$$

Player I wishes to maximize Eq. (C1); player II wants to minimize it. Therefore, I and II seek strategies that attain the outer extrema in the programs

$$\textit{Program I: } \underline{v} = \sup_{X:EX \leq a} \inf_{Y:EY \leq b} Pr\{X \geq Y + c\}, \tag{C2a}$$

$$\textit{Program II: } \bar{v} = \inf_{Y:EY \leq b} \sup_{X:EX \leq a} Pr\{X \geq Y + c\}. \tag{C3a}$$

If a strategy exists that attains the outer extrema for Program I (resp. II), it is called an *optimal strategy* for player I (resp. II). It is always true that $\bar{v} \geq \underline{v}$; if $\bar{v} = \underline{v}$, then the game is said to have a *value*, $v_0 = \bar{v} = \underline{v}$. A saddle-point solution to this game (if it exists) is a pair of allowable strategies, say (X_0, Y_0), such that

$$Pr\{X \geq Y_0 + c\} \leq Pr\{X_0 \geq Y_0 + c\} \leq Pr\{X_0 \geq Y + c\} \tag{C4}$$

is satisfied for all allowable (X, Y). The existence of a saddle-point is a sufficient condition for a value to exist; in this case we have

$$v_0 = \bar{v} = \underline{v} = Pr\{X_0 \geq Y_0 + c\} \tag{C5}$$

and thus X_0 (resp. Y_0) is an optimal strategy for player I (resp. player II).

In this appendix, we derive a unique saddle-point solution to Eq. (C3a). The special case $a = b = 1, c = 0$, has been studied by Bell and Cover [C2] in connection with competitive investment, and the special case $c = 0$ has been studied by McEliece and Rodemich [C3] as part of a study of optimal jamming of uncoded MFSK. We construct the general solution of Eq. (C2a) from the known solution in the special case $c = 0$. Without many of the complications that arise in the MFSK problem studied in Ref. C3 this special case admits a proof that is much simpler than that given in Ref. C3; we present this below.

Lemma 1: (Bell-Cover-McEliece-Rodemich) Consider the two-player, zero-sum game given by Eq. (C3a) when $c = 0$. This game has a value v_0 and unique saddle-point strategies $X_0 \sim F_0$ and $Y_0 \sim G_0$. These are given, in the case $a \geq b$, by†

$$v_0 = 1 - \frac{b}{2a}, \tag{C6a}$$

$$F_0(x) = U_{[0,2a]}(x), \tag{C6b}$$

$$G_0(x) = \left[\frac{b}{a}\right] U_{[0,2a]}(x) + \left[1 - \frac{b}{a}\right] \Delta_0(x); \tag{C6c}$$

* In this appendix, we abandon the convention, used earlier in the report, that distinguishes random variables with asterisks.

†Throughout this appendix we use the following notation: $X \sim F$ means that the real-valued random variable X has distribution function F. We denote by $U_{[a,b]}(x)$ the distribution function of a random variable that is uniformly distributed on the interval $[a,b]$, and we denote by $\Delta_c(x)$ the distribution function of the trivial random variable $X \equiv c$.

and, if $a < b$, are given by

$$v_0 = \frac{a}{2b}, \tag{C6d}$$

$$F_0(x) = \left[\frac{a}{b}\right] U_{[0,2b]}(x) + \left[1 - \frac{a}{b}\right] \Delta_0(x), \tag{C6e}$$

$$G_0(x) = U_{[0,2b]}(x). \tag{C6f}$$

Remark: The proof given here is a generalization of Bell and Cover's [C2].

Proof: Let $X \sim F$ and $Y \sim G$ be any allowable strategies. Observe that

$$Pr\{X \geq Y\} = \int_0^\infty G(x)\, dF(x) = 1 - \int_0^\infty F(x-)\, dG(x). \tag{C7}$$

First consider the case $a \geq b$. Let us show that (X_0, Y_0) satisfies Eq. (C4) when $c = 0$. Using the obvious inequality $U_{[0,d]}(x) \leq x/d$ when $x \geq 0$, we then obtain

$$\begin{aligned} Pr\{X \geq Y_0\} &= \int_0^\infty G_0(x)\, dF(x) \\ &= \left[1 - \frac{b}{a}\right] + \frac{b}{a} \int_0^\infty U_{[0,2a]}(x)\, dF(x) \\ &\leq \left[1 - \frac{b}{a}\right] + \frac{b}{2a^2} \int_0^\infty x\, dF(x) \\ &\leq 1 - \frac{b}{2a} = v_0. \end{aligned} \tag{C8}$$

In much the same way, using the right-most equality in Eq. (C7), we can show

$$Pr\{X_0 \geq Y\} \geq v_0. \tag{C9}$$

Since $Pr\{X_0 \geq Y_0\} = v_0$, we conclude that (X_0, Y_0) is a saddle-point and v_0 is the value of the game.

To complete the proof in the case $a \geq b$, it only remains to show the uniqueness of F_0 and G_0. First consider G_0. Let $Y_0' \sim G_0'$ be any other random variable such that $EY_0' \leq b$ and

$$Pr\{X \geq Y_0'\} \leq v_0, \tag{C10}$$

for all admissible X. Substitution of

(1): $X \sim U_{[0,2a]}(x)$,

(2): $X \sim \left[\frac{\beta}{\alpha+\beta}\right] \Delta_{a-\alpha}(x) + \left[\frac{\alpha}{\alpha+\beta}\right] \Delta_{a+\beta}(x)$,

for all $0 \leq \alpha, \beta \leq a$, into Eq. (C10) yields, respectively

(1): $G_0'(2a) = 1$,

(2): $\left[\frac{\beta}{\alpha+\beta}\right] G_0'(a-\alpha) + \left[\frac{\alpha}{\alpha+\beta}\right] G_0'(a+\beta) \leq v_0$,

for all $0 \leq \alpha, \beta \leq a$.

We claim that (2) implies that there is a line, say $l(x)$, that passes through the point (a, v_0) and is such that

$$G_0'(x) \leqslant l(x), \tag{C11}$$

for all $x \geqslant 0$. To prove this claim, define*

$$\mu \equiv \max_{0 \leqslant \beta \leqslant a} \frac{G_0'(a+\beta) - v_0}{\beta} < +\infty \tag{C12}$$

and let $\bar{\beta}$ attain the maxima. Let $l(x)$ be the line through (a, v_0) having slope μ. We know that $G_0'(a) \leqslant v_0 = l(a)$ (proof: take $\alpha = \beta = 0$ in (2)). By construction, $l(x)$ satisfies Eq. (C11) when $x \geqslant a$, and passes through the point $(a+\bar{\beta}, G_0'(a+\bar{\beta}))$. Now if

$$G_0'(a-\alpha) > l(a-\alpha), \tag{C13}$$

for some $0 \leqslant \alpha \leqslant a$, then α and $\bar{\beta}$ violate (2). Therefore, to avoid a contradiction, $l(x)$ must satisfy Eq. (C11) for $0 \leqslant x \leqslant a$ as well, proving the claim.

We now show that Eq. (C11) implies that $G_0' \equiv G_0$. For any measurable function, say $f(x)$, let ν_f denote the Lebesgue volume of the region in $\mathbf{R}^2$ comprising the points $R_f = \{(x,y) \mid 0 \leqslant x \leqslant 2a,\ f(x) \leqslant y \leqslant 1\}$. By an elementary fact of probability theory and (1), we know that

$$\nu_{G_0'} = EY_0' \leqslant b. \tag{C14}$$

Equation (C11) implies that $\nu_{G_0'} \geqslant \nu_l$, and hence

$$\nu_l \leqslant b. \tag{C15}$$

Since $l(0) \geqslant G_0'(0) \geqslant 0$, $l(2a) \geqslant G_0'(2a) = 1$ and $l(a) = v_0$, R_l is a triangular region and $l(0)$ must be such that $0 \leqslant l(0) \leqslant 2v_0 - 1$. By elementary geometry, we can show that

$$\nu_l = \frac{a(1 - l(0))^2}{2(v_0 - l(0))} \tag{C16}$$

for all $0 \leqslant l(0) \leqslant 2v_0 - 1$. It is easy to show that Eq. (C16) is a strictly decreasing function of $l(0)$ that attains a minimum value of $\nu_l - b$ when $l(0) = 2v_0 - 1$. Therefore the only line, $l(x)$, that passes through (a, v_0) and that does not contradict Eq. (C15) satisfies $l(0) = 2v_0 - 1$, and hence

$$l(x) = \frac{bx}{2a^2} + \left[1 - \frac{b}{a}\right]. \tag{C17}$$

Comparing Eq. (C17) with Eq. (C6c), we see that l equals G_0 for all x such that $0 \leqslant x \leqslant 2a$ and $0 \leqslant l(x) \leqslant 1$. It follows from Eq. (C11), the nonnegativity of Y_0' and Y_0, and (1), that

$$G_0'(x) \leqslant G_0(x)$$

for all real x. This implies that $G_0' \equiv G_0$, since if $G_0'(x) < G_0(x)$ for some $0 < x \leqslant 2a$, then

$$EY_0' = \nu_{G_0'} > \nu_{G_0} = b,$$

*The "max" in Eq. (C12) is justified because $(G_0'(a+\beta) - v_0)/\beta$ is upper semicontinuous, and the right hand inequality because this function is bounded by v_0/a (to prove take $\alpha = a$ in (2)).

a contradiction. We conclude that, in the case $a \geqslant b$, G_0 is unique. The proof that F_0 is unique, and the proofs for the case $a < b$, are similar. This completes the proof of Lemma 1. •

We now consider the game Eq. (C2a) when $c > 0$, and show that the solution in this case can be constructed from the known solution for the case $c = 0$. To see this, note that any nonnegative $X \sim F$ that satisfies $EX \leqslant a$ can be decomposed in the following way:

$$X = \begin{cases} c + Z & \text{w.p. } p \\ W & \text{w.p. } 1 - p \end{cases} \tag{C18}$$

where $p = 1 - F(c-)$ and $W \sim L$ and $Z \sim H$ are nonnegative real-valued random variables. The distribution functions L and H are given by

$$L(x) = \begin{cases} \dfrac{F(x)}{F(c-)} & -\infty < x < c \\ 1 & x \geqslant c \end{cases}$$

if $F(c-) > 0$, otherwise $L(x) = \Delta_0(x)$; and

$$H(x) = \begin{cases} 0 & -\infty < x < 0 \\ \dfrac{F(x+c) - F(c-)}{1 - F(c-)} & x \geqslant 0 \end{cases}$$

if $F(c-) < 1$, otherwise $H(x) = \Delta_0(x)$.

In terms of the new variables p, Z, and W, the cost function Eq. (C1) becomes

$$\begin{aligned} Pr\{X \geqslant Y + c\} &= p\ Pr\{Z + c \geqslant Y + c\} \\ &\quad + (1 - p)\ Pr\{W \geqslant Y + c\} \\ &= p\ Pr\{Z \geqslant Y\}. \end{aligned} \tag{C19}$$

Clearly, W has no effect on the cost function $Pr\{X \geqslant Y + c\}$, only our choice of p and Z influence it. The latter choice is constrained by

$$EX = (1 - p)\ EW + p(c + EZ) \leqslant a$$

or

$$EZ \leqslant \frac{a - (1 - p)\ EW}{p} - c,$$

so that the widest choice of Z is permitted when $W \equiv 0$ and

$$EZ \leqslant \frac{a}{p} - c \equiv \hat{a}(p).$$

Using this decomposition, we can reformulate Eq. (C2a) in the following way:

$$\textit{Program I } \underline{\nu} = \sup_{(p,Z)\, EZ \leqslant \hat{a}(p)} \inf_{Y\, EY \leqslant b} p\ Pr\{Z \geqslant Y\}, \tag{C20}$$

$$\textit{Program II: } \bar{\nu} = \inf_{Y\, EY \leqslant b} \sup_{(p,Z)\, EZ \leqslant \hat{a}(p)} p\ Pr\{Z \geqslant Y\}. \tag{C20}$$

Games Eqs. (C2a) and (C20a) are equivalent in the following sense: If X_0, p_0, and Z_0 are related as in Eq. (C18), then $\{(p_0, Z_0), Y_0\}$ is a saddle-point for Eq. (C20a) *if and only if* (X_0, Y_0) is a saddle-point for Eq. (C2a); and, of course, the resulting values of both games are the same. Therefore, solving Eq. (C20a) is entirely equivalent to solving Eq. (C2a).

Using Eq. (C20a), we can derive the only candidate saddle-point for Eq. (C2a) in the following way. Suppose that $\{(p_0, Z_0), Y_0\}$ is a saddle-point so that

$$p\ Pr\{Z \geqslant Y_0\} \leqslant p_0\ Pr\{Z_0 \geqslant Y_0\} \leqslant p_0\ Pr\{Z_0 \geqslant Y\} \tag{C21}$$

for all admissible $\{(p,Z), Y\}$. Then, in particular, we have

$$p_0\ Pr\{Z \geqslant Y_0\} \leqslant p_0\ Pr\{Z_0 \geqslant Y_0\} \leqslant p_0\ Pr\{Z_0 \geqslant Y\} \tag{C22}$$

for all (Z, Y) such that $\{(p_0, Z), Y\}$ is allowable. Ignoring momentarily the trivial possibility that $p_0 = 0$, Eq. (C22) implies that (Z_0, Y_0) must be a saddle-point of Eq. (C2a) with constants

$$a' = \hat{a}(p_0) \equiv \frac{a}{p_0} - c\,,\ b' = b\,,\ c' = 0\,. \tag{C23}$$

Since Eq. (C6a) gives the unique solution to Eq. (C2a) when $c = 0$, we conclude that (Z_0, Y_0) must have the distributions F_0 and G_0 obtained when the constants Eq. (C23) are substituted into Eq. (C6a). The corresponding value of this game, as a function of p_0, is

$$v_0(p_0) \equiv \begin{cases} p_0\left[1 - \dfrac{b}{2\hat{a}(p_0)}\right] & \hat{a}(p_0) \geqslant b \\ \dfrac{p_0\,\hat{a}(p_0)}{2b} & \hat{a}(p_0)\,,\ b\,. \end{cases} \tag{C24}$$

We now show that Eq. (C21) fixes a value for p_0 as well. If $\{(p_0, Z_0), Y_0\}$ is a saddle-point for Eq. (C20a), then the left-hand bound in Eq. (C21) implies that

$$v_0 = \max_{0 \leqslant p \leqslant 1} v_0(p)\,.$$

Using this, we may explicitly find the only possible saddle-point. The following facts will be useful:

FACTS:

(1): The maxima of $v_0(p)$ over the range $0 \leqslant p \leqslant 1$ is attained by

$$p_0 \equiv \begin{cases} \dfrac{a}{c}\left[1 - \sqrt{\dfrac{b}{2c+b}}\right] & a \leqslant c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}}\right] \\ 1 & a > c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}}\right] \end{cases} \tag{C25}$$

and note that $p_0 \leqslant a/c$ when $c > 0$.

(2): Define $g(p)$ on the interval $0 \leqslant p \leqslant a/c$ by

$$g(p) = 1 - \frac{b}{\hat{a}(p)} - \frac{bc}{2\hat{a}^2(p)}.$$

Then $g(p_0) = 0$ if $0 \leqslant p_0 < 1$, and $g(p_0) \geqslant 0$ if $p_0 = 1$.

(3): $\hat{a}(p_0) \geqslant b$ for all $a, b > 0$, and $c > 0$, where p_0 is as defined in Eq. (C25).

Therefore, based on facts (1) and (3), Lemma 1, and the comments above, the only possible saddle-point for the game Eq. (C20a) is p_0, $Z_0 \sim H_0$, and $Y_0 \sim G_0$ where p_0 is given in Eq. (C25) and

$$H_0(x) = U_{[0,2\hat{a})_{p_0})]}(x), \tag{C26a}$$

$$G_0(x) = \left[\frac{b}{\hat{a}(p_0)}\right] U_{[0,2\hat{a}(p_0)]}(x-c) + \left[1 - \frac{b}{\hat{a}(p_0)}\right]\Delta_0(x). \tag{C26b}$$

Remark: Note that $a > 0$ implies that $\hat{a}(p_0) \equiv \frac{a}{p_0} - c > 0$, so that Eq. (C26b) is always well-defined.

H_0 and G_0 are obtained by substituting p_0 above into Eq. (C23), substituting the resulting constants into Eq. (C6a), and taking $H_0 \equiv F_0$. The corresponding value of the game is

$$v_0 = \begin{cases} \dfrac{a}{c}\left[1 + \dfrac{b}{c}\left[1 - \sqrt{1 + \dfrac{2c}{b}}\right]\right] & a \leqslant c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}}\right] \\ 1 - \dfrac{b}{2(a-c)} & a > c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}}\right] \end{cases}.$$

We have shown that $\{(p_0, Z_0), Y_0\}$ is the only candidate for a saddle-point for the game Eq. (C20a); let us now verify that this is indeed a saddle-point. Let $\{(p,Z), Y\}$ be any admissible triple, and suppose that $Z \sim H$ and $Y \sim G$. Then

$$\begin{aligned} p\ Pr\{Z \geqslant Y_0\} &= p \int_0^\infty G_0(x)\, dH(x) \\ &= p\left[1 - \frac{b}{\hat{a}(p_0)}\right] + \frac{bp}{\hat{a}(p_0)} + \int_0^\infty U_{[0,2\hat{a}(p_0)]}(x)\, dH(x) \\ &\leqslant p\left[1 - \frac{b}{\hat{a}(p_0)}\right] + \frac{bp}{2\hat{a}^2(p_0)} \int_0^\infty x\, dH(x) \\ &\leqslant p\left[1 - \frac{b}{\hat{a}(p_0)}\right] + \frac{bp\hat{a}(p)}{2\hat{a}^2(p_0)} \\ &= p\left[1 - \frac{b}{\hat{a}(p_0)} - \frac{bc}{2\hat{a}^2(p_0)}\right] + \frac{ba}{2\hat{a}^2(p_0)} \\ &= p\, g(p_0) + \frac{ba}{2\hat{a}^2(p_0)} \end{aligned}$$

From fact (2) it follows that $pg(p_0) \leqslant p_0 g(p_0)$ and therefore

$$p\ Pr\{Z \geqslant Y_0\} \leqslant p_0\, g(p_0) + \frac{ba}{2\hat{a}^2(p_0)}$$

$$= p_0 \left[1 - \frac{b}{2\hat{a}(p_0)} \right] = v_0 .$$

The proof of

$$p_0\ Pr\{Z_0 \geqslant Y\} \geqslant v_0$$

for all allowable Y is similar to the proof of Lemma 1 and so is omitted.

We conclude that $\{(p_0, Z_0), Y_0\}$ is the unique saddle-point for Eq. (C20a) and that v_0 is the corresponding value. Recalling the equivalence between the games Eqs. (C20a) and (C2a) when p, Z, and X are related by Eq. (C18) (cf. remarks following Eq. (C20a)), we have therefore proved the following:

Theorem: Consider the two-player, zero-sum game given by Eq. (C2a). This game has a value v_0 and unique saddle-point strategies $X_0 \sim F_0$ and $Y_0 \sim G_0$. These are given in Lemma 1 for the case $c = 0$, and for the case $c > 0$ by

$$v_0 = \begin{cases} \dfrac{a}{c}\left[1 + \dfrac{b}{c}\left[1 - \sqrt{1 + \dfrac{2c}{b}} \right] \right] & a \leqslant c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}} \right] \\ 1 - \dfrac{b}{2(a-c)} & a > c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}} \right] \end{cases} \tag{C27a}$$

$$F_0(x) = p_0\, U_{[0,2\hat{a}(p_0)]}(x) + (1 - p_0)\, \Delta_0(x), \tag{C27b}$$

$$G_0(x) = \left(\frac{b}{\hat{a}(p_0)} \right) U_{[0,2\hat{a}(p_0)]}(x - c) + \left(1 - \frac{b}{\hat{a}(p_0)} \right) \Delta_0(x), \tag{C27c}$$

where $\hat{a}(p) = a/p - c$ and

$$p_0 = \begin{cases} \dfrac{a}{c}\left[1 - \sqrt{\dfrac{b}{2c+b}} \right] & a \leqslant c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}} \right] \\ 1 & a > c + \dfrac{b}{2}\left[1 + \sqrt{1 + \dfrac{2c}{b}} \right] \end{cases}$$

Remark: Note that some of the quantities above are indeterminant when $c = 0$. Nevertheless the saddle-point strategies and the value in Eq. (C27a) tend continuously to those of Lemma 1 as $c \to 0$. To see this, fix $a > 0$ and $b > 0$ and denote by $v_0(c)$, $X_0(c)$, and $Y_0(c)$, the value and saddle-points for the game Eq. (C2a) with parameters a, b, and c. As $c \to 0$, we have by elementary expansion

$$\sqrt{1 + \frac{2c}{b}} = 1 + \frac{c}{b} - \frac{c^2}{2b^2} + o(c^3),$$

and therefore

$$\frac{a}{c}\left[1 + \frac{b}{c}\left[1 - \sqrt{1 + \frac{2c}{b}} \right] \right] = \frac{a}{2b} + o(c).$$

We also have, trivially,

$$c + \frac{b}{2}\left[1 + \sqrt{1 + \frac{2c}{b}}\right] = b + o(c).$$

Therefore, we conclude that as $c \to 0$,

$$v_0(c) \to v_0(0),$$
$$X_0(c) \to X_0(0) \text{ (in law)},$$
$$Y_0(c) \to Y_0(0) \text{ (in law)},$$

as claimed.

END

11-86

DTIC