AD NUMBER

AD090352

CLASSIFICATION CHANGES

TO: unclassified

FROM: confidential

LIMITATION CHANGES

TO:

Approved for public release, distribution unlimited

FROM:

Controlling DoD Organization: Department of the Air Force, Attn: Public Affairs Office, Washington, DC, 20330.

AUTHORITY

USAF [per MIT Notice], Feb 1963; USAF [per MIT ltr], 11 Feb 1981

UNCLASSIFIED

AD 90352

DEFENSE DOCUMENTATION CENTER

FOR

SCIENTIFIC AND TECHNICAL INFORMATION

CAMERON STATION ALEXANDRIA, VIRGINIA

CLASSIFICATION CHANGED
TO UNCLASSIFIED
FROM SECRET
PER AUTHORITY LISTED IN

AUTHORITY USAF (per MIT notice
February 1963.)

UNCLASSIFIED

REPRODUCTION QUALITY NOTICE

This document is the best quality available. The copy furnished to DTIC contained pages that may have the following quality problems:

- Pages smaller or larger than normal.
- Pages with background color or light colored printing.
- Pages with small type or poor printing; and or
- Pages with continuous tone material or color photographs.

Due to various output media available these conditions may or may not cause poor legibility in the microfiche or hardcopy output you receive.

☐ If this block is checked, the copy furnished to DTIC contained pages with color printing, that when reproduced in Black and White, may change detail of the original copy.

BEST AVAILABLE COPY

SECRET

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

SOME NOTES ON JAMMING, I

(Title: UNCLASSIFIED)

W. L. ROOT

3 JANUARY 1956

TECHNICAL REPORT NO. 103

SECRET

SECRET

This document consists of 16 pages. No. 2 of 450 copies.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY
LINCOLN LABORATORY

SOME NOTES ON JAMMING, I
(Title: UNCLASSIFIED)

W.L. Root

Group 34

Technical Report No. 103

3 January 1956

LEXINGTON MASSACHUSETTS

SECRET

ABSTRACT

This report is a theoretical study of the problem of maintaining radio communications in the presence of electronic countermeasures. Specifically, certain idealized examples are considered in which the problem is to devise a detector, to be used with a certain type of signal, which is as little susceptible to countermeasures as possible. The criterion according to which performance is to be maximized is a game-theoretic one; the applicability of this point of view is discussed in Sec. I. In Sec. II definitions are stated. In Secs. III and IV some elementary theory is presented and three examples are worked out.

It is the intention of the author to follow this report with another on the same subject and the material of Secs. I and II is designed to serve as a foundation for this later report.

SOME NOTES ON JAMMING, I

I. INTRODUCTION

This report is a preliminary study, from an abstract point of view, of radio communications in the presence of jamming or electronic countermeasures. The discussion is, in fact, sufficiently abstract that it might apply to other communication problems, but all the motivating examples come from the field of radio communications. We restrict ourselves entirely to cases in which the messages are composed from two-letter alphabets (as is true for commercial teletype). This is done largely in order to obtain a simple treatment, but it is felt that not much is lost in idea in specializing from n-letter alphabets to two-letter alphabets.

In ordinary radio communications, reception is hampered by accidental interference, man-made and natural. Presumably man-made interference can be nearly eliminated if necessary. Natural interference cannot be eliminated, and its effects can be troublesome in certain circumstances. In studying methods of minimizing natural interference, much use has been made in late years of statistical methods. Thus receiver noise, although unpredictable, has well-known statistical properties which can be deduced largely from a theory of its origin; propagation disturbances caused by multiple paths or scatter phenomena are more difficult to get hold of theoretically, but still some statistical knowledge of their behavior can be gathered which is useful. In all such cases, something can be done to reduce natural interference or its effects because, although the precise behavior of nature may be unpredictable, trends and rough outlines of its future behavior may be established from a knowledge of its behavior in the past.

In military radio communications, reception may be hampered not only by accidental interference but also by intentional interference (jamming or electronic countermeasures). In some circumstances, particularly where communications are carried out over a short range, accidental interference may do negligible harm and the whole problem is that of combating countermeasures. In this report, we consider only this latter situation. There are some obvious differences between the situation with intentional interference and that with various forms of natural interference which we want to emphasize.

(a) In some signal-plus-noise problems, probability distributions governing the noise signal are known a priori. It seems meaningless to assign probability distributions a priori to any parameter governing a jammer's activity (except insofar as the jammer is expected to choose an optimum strategy in a sense to be made precise below).

(b) In communication problems involving multipath propagation, say, it seems plausible to test the propagation characteristics of the channel simultaneously with receiving a communication. Then empirical distributions of appropriate parameters of the channel can be obtained which may be of use in predicting its future variation. Although information about a jammer can be obtained simultaneously with receiving a jammed message, about the only value of this information is to show what the jammer can do, not what he will do or is likely to do. Of course, intelligence may be at hand describing the possible range of his activities, and this can be an advantage to the communicator.

(c) Natural interference may consist of the superposition of an unwanted signal (noise) on the wanted signal or it may consist of some other type of perturbation of the signal (as in multipath and scatter communication) or both. As yet, probably no one can jiggle the mechanism of propagation through the ionosphere and troposphere; so, for radio jamming, one need consider only the case where the interference consists of a jamming signal superposed on the communication signal.

We have first to consider the conceptual problem of how to approach the communication-through-jamming situation theoretically. We adopt the following point of view: it is desired to find from some limited choice of modulation-detection schemes one that will minimize the effect of the most harassing electronic countermeasures the enemy can use. The phrase "limited choice" is used simply because we do not hope to solve the problem in full generality; the phrase "can use" is meant to imply that there is some sort of limitation, usually a cost limitation, on the measures available to the enemy. This notion can be expressed in symbols. Suppose the modulation and detection schemes available can be indexed by a variable ξ, and the countersignal schemes available can be indexed by a variable η. Let M be a figure of merit for the communication; M is a function of ξ and η. Now, if ξ and η completely determine the mechanism of communication and the countersignal, then M is an ordinary (real-valued) function of ξ and η; if, on the other hand, ξ or η indexes a communication or countersignal "scheme" in the sense that it specifies a probability distribution for certain parameters which are allowed to vary, then M is a random variable. (The second use of the indices includes the first if one allows singular probability distributions.)

To get a numerical-valued figure of merit, one may take

$$\overline{M}(\xi,\eta) = E\left\{M(\xi,\eta)\right\}$$

In particular, let $M(\xi,\eta)$ be one if the signal is correctly received, and zero otherwise. Then

$$\overline{M}(\xi,\eta) = P(\xi,\eta)$$

is the probability of correctly receiving a signal; this is the figure of merit we shall use. Now, according to our intention as postulated above, we seek a ξ^* such that

$$\min_{\eta} P(\xi^*,\eta)$$

is as large as possible. Since the enemy does not know which ξ is chosen, he seeks an η^* such that

$$\max_{\xi} P(\xi,\eta^*)$$

is as small as possible. This formulation leads to notions already current in the theory of zero-sum two-person games, and we shall, in the sequel, adopt the terminology and use some results from this theory. We call the team of communicators player I and the enemy, player II. ξ and η are the mixed strategies of players I and II, respectively. $P(\xi,\eta)$ is the payoff function, and we may say that II pays I since it is for I's advantage to have $P(\xi,\eta)$ as large as possible, and to II's advantage to have $P(\xi,\eta)$ as small as possible. We let I_T designate the transmitter of the communication team and I_R designate the receiver. In the games we shall form with payoff function $P(\xi,\eta)$, the upper value of the game becomes the smallest probability of correct reception that the jammer can guarantee, and the lower value becomes the greatest probability of correct reception that the communicators can guarantee. A good strategy for player I specifies a communication scheme optimum within a given class of schemes; a good strategy for player II specifies a type of countermeasure optimum within a given class.

In the last paragraph, we have, in a rough general way, set up an abstract problem which is to represent the real-life communication-through-jamming problem. This formulation is not a thing to be proved or disproved mathematically; the author feels it is one reasonable formulation. The essential point is, of course, that we are adopting a minimax-type criterion.

How can one beat jamming? First, by finding the best communication system among those available so as to maximize the probability of correct reception per signal; second, by using repetition or some form of redundancy.

If the communicator is limited to systems in which, at best, he cannot get a satisfactory probability of correct reception per signal, then so long as this probability is strictly greater than one-half, by repeating the signal enough times he can get an over-all probability of correct reception as close to one as desired. Thus, if in a given situation one can find ξ^* such that $P(\xi^*,\eta) > 1/2 + \epsilon$ for all η, ideally the communicator can beat the jamming if he can afford the necessary redundancy. In practice, this means, of course, if his time-bandwidth product is sufficiently large. On the other hand, $P(\xi,\eta)$ can be raised, in general, if the number of available communication schemes can be enlarged; the communicator, by having more alternatives at hand, can force the jammer to "scatter his shot." This again means in practice, the greater the time-bandwidth product usable by the communicator, the better his chances of combating jamming. We shall discuss specific problems in Sec. IV of this report where $P(\xi^*,\eta)$ is very little greater than one-half and repetition is necessary. In Part II (to be published) we shall discuss "coded" systems (see Sec. II of this report) for which the redundancy is built in the form of a large number of alternatives for the communicators.

II. DEFINITIONS

A signal space is a set X closed under a commutative binary operation which we denote by +. A countersignal space is a subset Z of X. A message is a sequence of MARKS and SPACES. Given a signal space X and countersignal space Z, a communication from I_T to I_R comprises the following sequence: I_T is in possession of a message $\{\ell\}_n$, n = 1, ..., N, ℓ_n = MARK or SPACE, which he maps into a sequence $\{x_{n_i}\}_n$, n = 1, ..., N, i_n = 0, 1, of elements from X (or signals). II adds an element $z_n \in Z$ (or countersignal) to each x_{n_i}. I_R receives the sequence $\{x_{n_i} + z_n\}_n$, decides for each n whether $x_{n_i} + z_n$ represents a MARK or SPACE and translates his sequence of received signals into a message. It is understood in advance by I_R that x_{n_0} is to represent a SPACE at the nth place and x_{n_1} is to represent a MARK; i.e., the sequence of mappings used by I_T to go from M and S to the signal space are known to I_R. They are not necessarily known to II. II never knows when he adds z_n to x_{n_i} whether the i at the nth place is a zero or a one. There are two natural subcases of the class of communications described above. The first is the known fixed signal which is discussed in this report and the second is the coded signal to be described in Part II (to be published).

A. Known Fixed Signal

$x_{n_0} = x_0 \in X$ for every n and $x_{n_1} = x_1 \in X$ for every n. x_0 and x_1 are known to II as well as to I_R. Conventional radio telegraph or teletype systems belong in this category.

B. Coded Signal

x_{n_0} is, in general, different from x_{m_0}, $n \neq m$, and x_{n_1} is, in general, different from x_{m_1}. II does not know x_{n_0} and s_{n_1} for any n. Thus I_T and I_R must have a "code," not known to II, for ciphering messages into sequences of elements from X, and deciphering.

Fundamentally, detection is the process of translating elements from the signal space into MARKS and SPACES; it is the function I_R must perform on each received signal in order to reconstruct the message. However, we sometimes want to allow detection procedures which give a translation "either MARK or SPACE" or even "MARK with probability p or SPACE with probability (1 – p)" to some element of X. Such "detection" can be meaningful in cases where there is repetition or redundancy. Thus, a detector is represented mathematically as a functional on X taking on at least two and perhaps a continuum of values. However, for reasons that will become evident, we state a formal definition of detector, to be used below, in a slightly different form.

A detector is an n + 1-tuple $(f_1, \ldots, f_n, D)$ where $f_1, \ldots, f_n$ are real-valued functionals on X, and D is a decision-valued (taking on two or more values) function on the subset of R^n which is the image of $f_1, \ldots, f_n$. We shall sometimes call $(f_1, \ldots, f_n)$ the filter, and D the decision function. Two filters $(f_1, \ldots, f_n)$, $(g_1, \ldots, g_m)$ are equivalent for a given signal space X if for any decision function D to be used with $(f_1, \ldots, f_n)$ there is a decision function D' to be used with $(g_1, \ldots, g_m)$ which yields the same decision for every $x \in X$ and conversely.

Remark 1: Two filters $f = (f_1, \ldots, f_n)$ and $g = (g_1, \ldots, g_m)$ are equivalent if and only if for every x and $y \in X$ for which $f(x) = f(y)$, $g(x) = g(y)$, and vice versa.

Proof: Take D' as given by $D'[g(x)] = D[f(x)]$, $x \in X$. The proof that D' is a decision function is obvious.

III. EXAMPLES

Example 1: Keyed Carrier

This is a fixed signal system in which the presence of the RF carrier indicates a MARK and its absence indicates a SPACE. Precisely, the nth letter of the message is mapped into the zero function of t, $(n-1)T \leq t < nT$ if it is a SPACE and into, say, $A \cos \omega t$, $(n-1)T \leq t < nT$ if it is a MARK. For a per-signal analysis, we need consider only the interval [0, T], then $x_0 = 0$, $0 \leq t < T$, $x_1 = A \cos \omega t$, $0 \leq t < T$. The signal space X may be taken to be the class of all functions of integrable square on [0, T] (we write this $L_2[0, T]$), and the counter signal space Z to be a subset of X to be specified.

The choice of the signal space X is somewhat arbitrary in this example, or indeed in any fixed symbol system. The signals are real-valued functions of a real variable t over a finite interval [0, T] and obviously the countersignals should be also. Hence X will be a space of real-valued functions on [0, T]. The operation + should be ordinary pointwise addition of functions because the electromagnetic field components that the signals x and countersignals z represent add this way. X must include all functions of the form $x_i + z$, $i = 0, 1$, $z \in Z$ and, for convenience, we have required in our definition that $x_0, x_1 \in X$ and $Z \subset X$. It is convenient to choose X to be a linear space, and since the L_2-norm of a signal function can be interpreted immediately to be the energy of the signal, and since we shall suppose all signals to be of finite

energy, $L_2[0, T]$ will do as a choice for X. $L_2[0, T]$ is really too large, but for the fixed signal case this does not matter very much, for it means only that the filter of the detector be defined on an unnecessarily large domain. The choice of the countersignal space Z is more delicate since it reflects the latitude we allow the opponent, player II. It is reasonable to suppose that II is limited to a finite energy a per signal, so every $z \in Z$ must satisfy

$$\int_0^T z^2(t)\, dt \leq a^2 \quad .$$

We could let this be the only restriction on z (we do this in a later example) and so take Z to be the subset of $L_2[0, T]$ contained in the sphere of radius a. However, here we further restrict Z; in fact we require in addition that

$$\int_0^T z(t)\, x_1(t)\, dt = 0$$

for every $z \in Z$. The motivation for this requirement is as follows: in practice T is likely to include a great many periods of $\cos \omega t$ so that signals of different frequency will be nearly orthogonal to $\cos \omega t$. Even if the enemy attempts to send a signal with a $\cos \omega t$ component and his frequency is slightly off or there are occasional phase drifts due to shifting propagation conditions, then his countersignal will still actually be nearly orthogonal to $\cos \omega t$ over $[0, T]$. Note that this is equivalent to saying that we may expect the energies of the signal and countersignal to add. To avoid giving an unrealistic advantage to the communicators, we shall require, when we discuss detectors for the keyed-carrier type of communication, that the receiver is no better able to duplicate the phase and frequency of the transmitter carrier than is the jammer.

Example 2: Frequency-Shift Keying

This is a fixed-signal system in which

$$\left.\begin{aligned} x_0 &= x_0(t) = A \cos \omega_0 t \\ x_1 &= x_1(t) = A \cos \omega_1 t \end{aligned}\right\} 0 \leq t < T \quad .$$

We shall suppose what is nearly true if $\omega_0 \neq \omega_1$, that $\cos \omega_0 t$ and $\cos \omega_1 t$ are orthogonal over $[0, T]$. We again take $L_2[0, T]$ for X, and for Z we take that subset of X consisting of elements z which satisfy:

$$\int_0^T z^2(t)\, dt \leq a$$

$$\int_0^T z(t) \cos \omega_0 t\, dt = 0$$

$$\int_0^T z(t) \cos \omega_1 t\, dt = 0 \quad .$$

The justification of these choices of X and Z is the same as in Example 1.

Example 3: Correlation Detection

We want to consider both a fixed-signal system and a coded-signal system. In the fixed-signal system [Example 3 (a)] we take

$$\left.\begin{aligned} x_0 &= -x(t) \\ x_1 &= x(t) \end{aligned}\right\} 0 \leqslant t < T \quad , \qquad \text{Example 3(a)}$$

$X = L_2[0, T]$ and Z that subset of X consisting of all elements z satisfying

$$\int_0^T z^2(t)\, dt \leqslant a \quad .$$

We call this example the "correlation detection system" because the phase sensitivity of the detector required by the type of signals postulated is conventionally obtained by using a so-called correlation detector. It will turn out that this example is ideally a natural one, since only linear filters need be considered in the detector.

Example 3(b) is the same as 3(a) except that X, and hence Z, is to be further restricted and

$$\left.\begin{aligned} x_{n_0} &= -x_n(t) \\ x_{n_1} &= x_n(t) \end{aligned}\right\} (n-1)\, T \leqslant t < nT \quad , \qquad \text{Example 3(b)}$$

where $x_n(t) \in X$ and is not known to the enemy. We shall specify X and Z in the section devoted to this example.

IV. FIXED-SIGNAL CASE

For fixed-signal communication, the communicators have freedom only to specify a receiver or detector in an effort to outwit the jammer. This is the case discussed in this section.

The appropriateness of the mathematical notion of a game in the study of communication through jamming was argued in the introduction. For convenience, we now introduce the term D-game to mean a zero-sum two-person game which has a payoff function taking on values only between zero and one, including zero and one.

The games we discuss are D-games in which there is a one-to-one correspondence between pure strategies for II and countersignals z and, in this section, between pure strategies for I and detectors D. To be succinct we shall refer to a "strategy z (or D)." If in a particular context D = (f, d) and the filter f is fixed while the decision function d is free, we shall refer to a "strategy d." Before investigating the examples introduced in the preceding section, we set down precisely a few rather obvious general facts about the kind of game we are considering. We use a simple concept of equivalence between games;* briefly, (1) games G and G' are

*See Blackwell and Girshick, Theory of Games and Statistical Decisions (John Wiley, New York, 1954), p.11 for a formal definition.

equivalent if an elimination of duplicated strategies for either one of I or II in G yields G', and (2) G and G' are equivalent if there is a finite chain G, G_1, G_2, ..., G_n, G' such that each adjacent pair satisfies (1). This sort of equivalence preserves lower value v_*, upper value v^*, and value v (if it exists). We are especially concerned with lower value because it is the highest probability of being correct that I can guarantee himself.

Remark 1: If $f \sim g$, then for any D-game with fixed filter f, there is an equivalent D-game with fixed filter g.

Proof: It is obvious. We say the filter f is finer than the filter g with respect to X if for every x, $y \in X$ for which $g(x) \neq g(y)$, $f(x) \neq f(y)$.

Remark 2: If f is finer than g, there exists a filter $\tilde{g} \sim g$ such that for every ξ in the image of $\tilde{g}$ there exists an $x_\xi \in \tilde{g}^{-1}(\xi)$ for which

$$f(x_\xi) = \tilde{g}(x_\xi) \quad .$$

Proof: Choose x_ξ to be any point in $g^{-1}(\xi)$. Define $\tilde{g}$ by

$$\tilde{g}[g^{-1}(\xi)] = f(x_\xi) \quad .$$

$\tilde{g}$ obviously satisfies the statement. We shall say f contains $\tilde{g}$.

Remark 3: If f is finer than g, given any set S of strategies for II, if there exists a D-game using S and g with lower value v_*, then there exists a D-game using S and f with lower value $v'_* \geq v_*$.

Proof: Choose $\tilde{g} \sim g$ and contained in f by 2. Let G be the game using S and g. Then by 1, there is a game $\tilde{G}$ using S and $\tilde{g}$ equivalent to G, and hence with lower value v_*. Now form a D-game G' using S and f where a subset of I's strategies are obtained as follows: for each $\tilde{d}$ in $\tilde{G}$ define d' in G' by $d'[f(x)] = \xi$ if $x \in \tilde{g}^{-1}(\xi)$. Then I has available in G' every strategy he had available in $\tilde{G}$, hence the assertion.

Remark 4: Let f contain g, and x_0 and x_1 be fixed. Let $\tilde{X} \subset X$ be the set of points on which f and g agree. Suppose there exists $\tilde{Z} \subset Z$ such that

(a) $x_0 + z \in \tilde{X}$ for all $z \in \tilde{Z}$, $x_1 + z \in \tilde{X}$ for all $z \in \tilde{Z}$.

(b) For every ξ for which $x_0 + z \in g^{-1}(\xi)$ for some $z \in Z$, there exists $\tilde{z} \in \tilde{Z}$ such that $x_0 + \tilde{z} \in g^{-1}(\xi)$.

The same condition exists with x_0 replaced by x_1. Then given a D-game G with II's strategies any subset S of Z, with any set of strategies for I using f and with lower value v_*, there exists a D-game G' with I using g with lower value $v'_* \geq v_*$.

Proof: Restrict G by allowing II pure strategies only from $S \cap \tilde{Z}$. Call this restricted game $\tilde{G}$. Then the lower value $\tilde{v}_*$ of $\tilde{G}$ is not less than v_*. Since in $\tilde{G}$ the only elements of X that can occur are of the form $x_i + z$, $i = 0, 1$, and for these f and g take on the same values, I can replace f by g and his set of strategies remains unchanged. Thus $\tilde{G}$ can be realized with I using g. Finally if II now replaces the strategies $S \cap \tilde{Z}^C$ a game G' is formed equivalent to $\tilde{G}$, since each strategy in $S \cap \tilde{Z}^C$ is equivalent to one in $S \cap \tilde{Z}$. Hence $v'_* \geq v_*$.

Remark 3 makes the obvious point that if the communicator allows himself more complicated detectors, he will not lose anything. Remark 4 shows that in special circumstances there is a kind of complication that also will not gain him anything provided, of course, that the enemy uses his wits.

We have need in the sequel to bound the value of a game from above. The following very simple estimate is useful.

Remark 5: Let Γ be a zero-sum two-person game with payoff function $P(\alpha, \beta)$ defined on the rectangle $[0, a] \times [0, b]$, α denotes a pure strategy for player I, β for II; G denotes a mixed strategy (Stieltjes measure) for I, F for II. We suppose II pays I. Then if there exists a measure F_0 such that

$$\int P(\alpha, b)\, dF_0(\beta) \leq k \quad ,$$

for all $\alpha, v_* \leq k$.

Proof: $v_* = \sup_G \inf_F \int dG(\alpha) \int P(\alpha, \beta)\, dF(\beta)$.

Let G_ϵ be a strategy such that

$$\int dG_\epsilon(\alpha) \int P(\alpha, \beta)\, dF(\beta) \geq v_* - \epsilon \text{ for all } F \quad .$$

Then in particular,

$$v_* - \epsilon \leq \int dG_\epsilon(\alpha) \cdot k = k \quad .$$

This relation is independent of E, hence $v_* \leq k$.

Keyed Carrier (Example 1 of Sec. III)

We have already assumed that any countersignal available to II is orthogonal to $x_0(t)$ on $[0, T]$. This assumption was not made to simplify the problem, for it does not. Indeed, Example 3 is essentially the same as this one with this assumption removed. It was made to cover cases in which it is unrealistic to suppose that the enemy can duplicate the frequency and phase of the carrier signal. In such a case, the receiver could ideally tune out the countersignal and perfect communication would result. But this is unrealistic (unless we are dealing with an inferior enemy). So we suppose that there is a (narrow) band of frequencies containing the carrier frequency which the receiver cannot tune out, and, in fact, which the receiver cannot further decompose which is available to II. That is, we shall suppose that the only characteristics of a signal appearing in this band which the receiver can determine are those that are functions of amplitude.

The situation may be idealized as follows: Let $L(x_2)$ be the linear subspace of $L_2[0, T]$ generated by x_2, let M be a linear subspace of $L_2[0, T]$ containing $L(x_1)$ and let N be the orthogonal complement of $L(x_1)$ in M. We shall suppose that if x and y both belong to M and

$$||x||_2 = \left\{\int_0^T x^2(t)\,dt\right\}^{1/2} = \left\{\int_0^T y^2(t)\,dt\right\}^{1/2} = ||y||_2$$

then for any available filter f, $f(x) = f(y)$.

Let the filter f_0 be defined as follows:

write $y \in L_2[0, T]$ as $y = y_M + y_S$, where $y_M \in M$, $Y_s \in M^C$ (the orthogonal complement of M in $L_2[0, T]$), then $f_0(y) = ||y_M||_2^2$.

Remark 6: Let f be any filter containing f_0. Then the conclusion of Remark 4 holds with $g = f_0$.

Proof: By hypothesis f and f_0 agree on M so $\tilde{X} = M$. Let $\tilde{Z} = N$. Then the conditions 4(a) and 4(b) are satisfied.

Thus, within the restriction that we have set, the simple filter which projects on a linear subspace and then determines norm is as good as any against jamming. The obvious physical device to approximate this abstract "filter" is a flat bandpass filter (filter in the usual sense) followed by a square-law device. We may now, in this example, confine our attention to D-games in which I uses f_0 and II takes all his pure strategies from N. The decision functions used by I will have for domain some subset of the positive real line; in particular, if we take $||x_1||_2 = 1$ and limit II's power, i.e., consider only z for which $||z||_2^2 \leq a$, the domain of the decision functions will be the interval $[0, a + 1]^2$. We now use Remark 5 to find an upper bound on v_* for any D-game in which I uses f_0 and II uses strategies from N. Notice that II may confine his strategies to a one-dimensional linear subspace of N and hence that his strategies may be indexed by the set of real numbers $[0, a]$.

Remark 7: Let G be a D-game with x_0 and x_1 as specified in this section in which I uses the filter f_0 and II's strategies are of the form αz_0, $z_0 \in N$, α a real number, where $||(z_0)||_2^2 \leq a$. Then the lower value of G is less than or equal to $1/2 + 1/2a$.

Proof: Let $||z_0||_2 = 1$, and map II's strategies onto the interval $[0, a]$ by carrying $\alpha z_0 \to \alpha$. Let d_β be the decision function corresponding to any particular strategy β of I. Then if II uses the pure strategy α, the payoff is

$$\frac{d_\beta(\alpha + 1) + [1 - d_\beta(\alpha)]}{2}.$$

Hence,

$$\frac{1}{a}\int_0^a P(\beta, \alpha)\,d\alpha = \frac{1}{2a}\int_0^a \left\{d_\beta(\alpha + 1) + [1 - d_\beta(\alpha)]\right\}\,d\alpha \leq \frac{1}{2} + \frac{1}{2a}$$

for all β. The conclusion follows from Remark 5.

Remarks 6 and 7 together assure us that in a fixed-signal keyed-carrier system with ratio of jamming power to signal power equal to a and under the restrictions on receiver and jammer which were imposed, the communicators cannot guarantee themselves a probability per symbol of being correct greater than $1/2 + 1/2a$.

We now exhibit a particular game of the type being discussed which has a value nearly achieving this bound. A good mixed strategy for I in this game, one of which we shall show, specifies a nearly optimum detection scheme for the communicators.

For any $\beta \geq 1$ we define d_β as follows:

$$d_\beta(s) = 0, \quad 0 \leq s < \beta$$

$$= 1, \quad \beta \leq s \quad .$$

That is, we call the signal a MARK if the output of the filter is greater than or equal to β, and a SPACE otherwise. The pure strategy β for I is then the strategy corresponding to the detector (f_0, d_β). Since the received signal is of the form $y = x_i + \sqrt{\alpha}\, z_0$, $f_0(y) = \delta + \alpha$, $\delta = 0$ if x_0, $\delta = 1$ if x_1, $0 \leq \alpha \leq a$. It follows then that for strategy β for I, the payoff as a function of α is given by

$$0 \leq \alpha < \beta - 1 \qquad P = \frac{1}{2}$$

$$\beta - 1 \leq \alpha < \beta \qquad P = 1$$

$$\beta \leq \alpha \leq a \qquad P = \frac{1}{2} \quad .$$

We shall call this game G_1. It follows from a general theorem that this game has a value,* however, we shall show this fact directly. If a game G_1' is formed from G_1 by removing some of I's strategies while leaving II's strategies unchanged, and if G_1' has a value v', then $v' \leq v_*$, the lower value of G_1; similarly, if a game G_1'' is formed from G_1 by removing some of II's strategies while leaving I's strategies unchanged, and if G_1'' has a value v'', then $v'' \geq v^*$. We shall find finite games G_1' and G_1'', which therefore have values, such that $v' = v'' = v$. Good strategies for G_1' and G_1'' are then good strategies for G_1. This technique amounts to no more really than making a shrewd guess at good strategies and then testing them.

If $n - 1 \leq a < n$, n a positive integer, form G_1' by allowing I the set of pure strategies $\{1, 2, \ldots, n\}$, i.e., $\beta = 1$, $\beta = 2$, etc. The resulting game is easily seen to be equivalent to a finite game with the following payoff matrix.

II \ α \ I \ β					
	$\frac{1}{2}$	. . .	$\frac{1}{2}$	1
	$\frac{1}{2}$	. . .	1	$\frac{1}{2}$
	.	. . .	.	.
	1	$\frac{1}{2}$ . . .		$\frac{1}{2}$

This game has value

$$v' = \frac{n-1}{n} \cdot \frac{1}{2} + \frac{1}{n} = \frac{1}{2} + \frac{1}{2n} \quad ,$$

*S. Karlin, Contributions to the Theory of Games (Princeton University Press, 1950); Vol. I, "Operator Treatment of Minimax Principle."

and a good mixed strategy for I is that which weights evenly each pure strategy. Form G_1'' by allowing II the set of pure strategies 0, 1, ..., n − 1. G_1'' is easily seen to be equivalent to a finite game with exactly the same payoff matrix as above; hence

$$v'' = \frac{1}{2} + \frac{1}{2n} = v \quad .$$

To summarize, the detection scheme specified by (f_0, d_β) where β is chosen randomly with a uniform distribution from the integers 1, ..., n, $n - 1 \leq a < n$, where f_0 and d_β are as defined above will guarantee the communicators a per-signal probability of being correct of $1/2 + 1/2n$. No other available filter will do better than f_0, and no decision scheme exists which will make the probability greater than $1/2 + 1/2a$. Whether or not this value can be achieved is left an open question.

Frequency-Shift Keying (Example 2 of Sec. III)

The discussion concerning the previous example is largely applicable here. We let $L(x_i)$, i = 0, 1, be the linear subspace of $L_2[0, T]$ generated by x_i; M_i, i = 0, 1, be a linear subspace properly containing $L(x_i)$, and N_i, i = 0, 1, be the orthogonal complement of N_i in M_i. We suppose M_0 is orthogonal to M_1 and that Z is a subset of $N_1 + N_0$. Let $\hat{f}$ be a filter defined as follows: $\hat{f} = (f_0, f_1)$, where $f_0(x)$ and $f_1(x)$ are the norms of projections onto M_0 and M_1, respectively. That is, f_0 and f_1 are defined exactly as was f_0 in the previous example.

Remark 8: Let f be any filter containing $\hat{f}$. Then the conclusion of Remark 4 holds with $g = \hat{f}$.

Proof: Let the $\tilde{Z}$ of Remark 4 be $N_0 = N_1$.

In this example there are two reasonable constraints on jamming power: (1) the total power in both MARK and SPACE channels may be limited and (2) the power in each channel may be limited individually. In either case, we can get an upper bound on v_* in the same way as in the preceding example.

Remark 9: Let G be any D-game in which II uses strategies $z = \alpha z_0 + \beta z_1$, $z_0 \in N_0$, $z_1 \in N_1$, $||\alpha z_0||_2^2 \leq a$, $||\beta z_1||_2^2 \leq a$, and in which I uses $\hat{f}$. Then

$$v_* \leq \frac{1}{2} + \frac{1}{a} - \frac{1}{2a^2} \quad .$$

Proof: Let $d(y_0, y_1)$ be a decision function, then by Remark 5,

$$v_* \leq \frac{1}{a^2} \int_0^a \int_0^a \left\{ \frac{d(z_0 + 1, z_1) + 1 - d(z_0, z_1 + 1)}{2} \right\} dz_0 dz_1$$

$$\leq \frac{1}{2} + \frac{1}{a} - \frac{1}{2a^2} \quad .$$

The same bound can be obtained in essentially the same way if the constraint $||z||_2^2 = a$ is imposed. It would seem that I ought to be able to guarantee himself a higher payoff in this example than in the first one, and the above estimate of v_* perhaps strengthens this supposition. I have not yet, however, worked out a game showing this. It is trivial to describe a game and strategy

in which v is asymptotically $1/2 + 1/2a$. In fact, if MARK and SPACE are detected independently, each as in Example 1, there are available after each signal two judgments as to what the signal was. If (M, M) is called M, (S, S) is called S, and (M, S) and (S, M) are called no decision (equally probable MARK or SPACE) then the payoff is exactly as in Example 1.

Thus, for the idealized FSK, we can specify an optimum filter and a mixed decision function that will guarantee exactly as good detection as guaranteed by the detector specified for the previous example. The question of a best or even an asymptotically best mixed decision function is left open.

Correlation Detection (Example 3 of Sec. III)

In this example we suppose that the receiver can duplicate not only the form of the transmitted signal but also its phase. In order to make the situation interesting, we suppose that the enemy can do the same. Again $X = L_2[0, T]$ with + being ordinary linear space addition; Z is a subset of $L_2[0, T]$, and the only restriction that need be imposed on Z is that $||z||_2^2 \leq a$, $z \in Z$. We assume $x_1 = x(t)$, $0 \leq t < T$,

$$\int_0^T x^2(t)\, dt = 1 \quad ,$$

and $x_0 = -x(t)$. Let $\tilde{f}$ be the filter defined by

$$\tilde{f}(y) = \int_0^T x(t)y(t)\, dt \quad .$$

This filter is as good as any from our point of view.

Remark 10: Let f be any filter containing $\tilde{f}$. Then the conclusion of Remark 4 holds with $g = \tilde{f}$.

Proof: Let the $\tilde{Z}$ of Remark 4 be the one-dimensional linear space spanned by x_1.

Remark 11: Let G be any D-game in which II uses strategies $z = ax_1$, $a^2 \leq a$, and in which I uses $\tilde{f}$. Then

$$v_* \leq \frac{1}{2} + \frac{1}{2\sqrt{a}} \quad .$$

Proof: Let d(y) be a decision function, then by Remark 5

$$v_* \leq \frac{1}{2\sqrt{a}} \int_{-\sqrt{a}}^{+\sqrt{a}} \frac{d(z+1) + 1 - d(z-1)}{2}\, dx$$

$$\leq \frac{1}{2} + \frac{1}{2\sqrt{a}} \quad .$$

We now construct a D-game in which II can guarantee himself a probability of being correct which is asymptotically equal to the upper bound established in Remark 11.

Let I use the filter $\tilde{f}$. Then since $\tilde{f}(y)$ is a real number for any $y \in X$, the domain of definition of the decision functions to be used by I is the real line. For each $\beta \geq 0$ define a decision function d_β as follows:

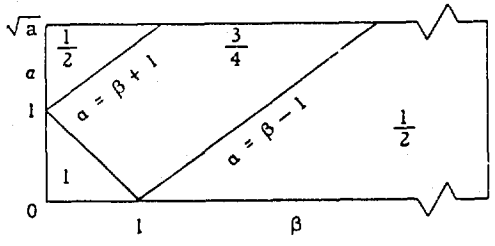
$$d_\beta(\xi) = 0 \quad , \qquad \xi < -\beta$$
$$= \tfrac{1}{2} \quad , \qquad |\xi| \leq \beta$$
$$= 1 \quad , \qquad \xi > \beta \quad .$$

Players I's set of strategies is the interval $[0, \infty]$; choice of strategy β, $\beta \in [0, \infty]$ means that player I uses the detector $(\tilde{f}, d_\beta)$. Player II chooses a counter signal ax_1, $a^2 \leq a$. Since $x = x_0$ or x_1 each with probability one-half, it will be evident that the sign of a is immaterial. II's set of strategies is the interval $[0, \sqrt{a}]$. The payoff P as a function of a and β is given by the following table.

$\beta < 1$	$0 \leq a < 1 - \beta$	$P = 1$
$\beta < 1$	$1 - \beta \leq a \leq 1 + \beta$	$P = 3/4$
$\beta < 1$	$1 + \beta < a$	$P = 1/2$
$\beta \geq 1$	$0 \leq a \leq \beta - 1$	$P = 1/2$
$\beta \geq 1$	$\beta - 1 < a \leq \beta + 1$	$P = 3/4$
$\beta \geq 1$	$\beta + 1 < a$	$P = 1/2$

A diagram of the "matrix" of the game is:

Player II's Strategies



Player I's Strategies

where the values of the payoff on the dividing lines are given by continuity to the left. That this game has a value can be shown by Karlin's theorem.*

We list some conclusions about this game, all of which can be obtained from elementary arguments:

(1) The value v of the game is monotonic nonincreasing as a becomes larger. This is true because, given $a < a_2$, the game with a_1 is a reduction of the game with a_2 obtained by restricting II's strategies but not restricting I's.

(2) If $a < 1$, $v = 1$ and a good pure strategy for I is d_0.

(3) If $2n - 1 < \sqrt{a} < 2n + 1$, $n = 1, 2, \ldots$, an upper bound for the value of the game is $1/2 + 1/4n$. To show this take $a_1 = 1$, $a_2 = 3$, $a_n = 2n - 1$. The resulting reduced game is equivalent to a finite game for which the value is easily seen to be $1/2 + 1/4n$.

*See footnote, p. 10.

(4) If $2n - 1 \leqslant \sqrt{a} < 2n$, $n = 1, 2, \ldots$, a lower bound for the value of the game is $1/2 + 1/4n$. To show this, take $\beta_1 = 1 - (2n - \sqrt{a})$, $\beta_2 = 3 - (2n - \sqrt{a})$, $\ldots$, $\beta_n = (2n - 1) - (2n - \sqrt{a}) = \sqrt{a} - 1$. The resulting reduced game has value $1/2 + 1/4n$. A good strategy for I is the mixed strategy which assigns weight $1/n$ to each β_i. It follows from (1) that $1/2 + 1/4n$ is also a lower bound for the value of the original game if $2n - 1 \leqslant \sqrt{a} < 2n - 1$. It is easily verified that in this case if $\sqrt{a}$ is replaced by $\sqrt{a} + 1$ in β_i, the same strategy as given above guarantees a payoff of $1/2 + 1/4n$.

(5) It follows from (1), (3) and (4) that the actual value of the game is $1/2 + 1/4n$ if $2n - 1 \leqslant \sqrt{a} < 2n$, $n = 1, 2, \ldots$, and that the value lies between $1/2 + 1/4n$ and $1/2 + 1/[4(n + 1)]$ if $2n \leqslant \sqrt{a} \leqslant 2n + 1$.

It will be noticed that the communicators have an advantage in this case as compared with the first example; roughly, they can get a probability of $1/2 + 1/2\sqrt{a}$ as compared with $1/2 + 1/2a$. In all of these examples, the best guaranteed probability of being correct approaches $1/2$ as the jamming power becomes infinite.