KYBERNETIKA — VOLUME 25 (1989), NUMBER 3

# ABOUT OPTIMUM SIGNALLING OF INFORMATION

IGOR VAJDA

Signal alphabets for information transmission through noisy wave channels and their optimum demodulation are considered. Explicit formulas for demodulation risk are obtained in case the channel is Gaussian. Optimization of signal alphabets with respect to the demodulation risk, as well as with respect to other information-theoretic criteria (Shannon information, capacity, cutoff rate), is studied. These criteria may lead to different alphabets. Quite paradoxically, one of these alphabets may decrease the cutoff rate of the other by almost 100% and, at the same time, the demodulation risk also by almost 100%. The risk and capacity (or Shannon information) display similar paradox but with the percentage level of about 40%. Practical consequences are deduced from these circumstances. Some interesting open problems are outlined.

## 1. SIGNAL ALPHABETS AND DEMODULATION

We consider a discrete information source able to deliver every $T$ seconds one of $M$ information symbols $\{1, \ldots, M\}$, where $M \geqq 2$. Transmission of information produced by the source usually consists of the following steps.

(a) The transmitter modulates a waveform depending on the information symbol delivered by the source. The waveform is assumed to be a real valued Lebesgue square-integrable function defined on the interval $[0, T]$. A family

$$\mathscr{S} = (S_i(t) \mid i = 1, \ldots, M)$$

of waveforms corresponding in a one-to-one way to the information symbols is assumed to be designed in advance. This set, called the *signal alphabet*, is supposed to satisfy for some $E > 0$ the condition

$$c_{ii} = E\,, \quad i = 1, \ldots, M\,.$$

Here $c_{ii}$ are diagonal elements of an $M \times M$-matrix $\boldsymbol{C}$, called the *configuration matrix* of the alphabet $\mathscr{S}$, with the general element

$$c_{ij} = \int_0^T S_i(t)\, S_j(t)\, \mathrm{d}t\,.$$

The quantity $E$ is an *energy* of the alphabet. Hence the modulation reduces to a simple choice of waveforms from $\mathscr{S}$ and their subsequent sending through a channel which is assumed to connect the transmitter with the receiver.

(b) The channel is supposed to be of a waveform nature too. It operates by adding to the transmitted waveform a *random noise* waveform. The additive random noise waveform is assumed to be a generalized zero-mean random process $(X(t) \mid 0 \leqq t \leqq T)$. As well known, this means that there is a linear mapping $I$ from the Banach space $L_2$ of real functions $S = (S(t) \mid 0 \leqq t \leqq T)$ to the space of zero-mean real random variables. The values $I(S)$ are interpreted as correlations between signals $S$ and the process trajectories, i.e.

$$\int_0^T S(t)\, X(t)\, \mathrm{d}t \triangleq I(S)\,, \quad S \in L_2\,,$$

(c) The receiver observes a random waveform, i.e. a realization of a real valued random process $(Y(t) \mid 0 \leqq t \leqq T)$. This process is defined by

$$Y(t) = S_i(t) + X(t)\,, \quad 0 \leqq t \leqq T,$$

under the condition that the $i$th information symbol is transmitted. Thus the receiver has at its disposal a statistical experiment described by the Kolmogorov's sample space $(\mathbb{R}^{[0,T]}, \mathscr{B}^{[0,T]})$ of real valued random processes with the time domain $[0, T]$ and by a family $(\nu_i \mid i = 1, \ldots, M)$ of measures on this space defined as sample measures of the process $(S_i(t) + X(t) \mid i = 1, \ldots, M)$. We shall restrict ourselves to the *correlation demodulation* (cf. Chap. 8 in [3]) where, instead of the process $(Y(t) \mid 0 \leqq t\ T)$, the receiver observes only the vector-valued statistic

$$\boldsymbol{Z} = (Z_1, \ldots, Z^M) = \left(\int_0^T S_1(t)\, Y(t)\, \mathrm{d}t,\ \ldots,\ \int_0^T S^M(t)\, Y(t)\, \mathrm{d}t\right). \tag{1}$$

In this case the receiver's statistical experiment has the Euclidean sample space $(\mathbb{R}^M, \mathscr{B}^M)$ and a family $(\mu_i \mid i = 1, \ldots, M)$ of probability measures on it, where

$$\mu_i = \nu_i \boldsymbol{Z}^{-1}\,. \quad i = 1, \ldots, M\,.$$

The demodulation itself is a measurable mapping $\Delta$ from the sample space $\mathbb{R}^M$ into a decision space $\mathscr{D} = \{1, \ldots, M'\}$ where $M' \geqq M$. The receiver's decisions are said *hard* if $M = M'$ and *soft* if $M' > M$. In the case of hard decisions the event $\Delta(\boldsymbol{Z}) = i \in \mathscr{D}$ is interpreted that the $i$th information symbol was transmitted. In the case of soft decision with $M' = 2M$ the event $\Delta(\boldsymbol{Z}) = i \in \{1, \ldots, M\}$ is interpreted as above and the event $\Delta(\boldsymbol{Z}) = M + i$ may have the same interpretation, but with the appendix: "this decision is unreliable". Another possibility is to interpret all decisions from the set $\{M + 1, \ldots, M + M\}$ as an erasure of the transmitted information symbol – in this case it suffices to take $\mathscr{D} = \{1, \ldots, M, M + 1\}$. One may also consider $M' = rM$ with $r - 1$ different levels of unreliability etc.

The following fact is frequently used in the sequel.

**Proposition 1.** For every $i = 1, \ldots, M$, $\mu_i$ is the sample probability measure of the random vector $\boldsymbol{c}_i + \boldsymbol{W}$ where $\boldsymbol{c}_i$ is a deterministic vector defined as the $i$th row of the

configuration matrix $\boldsymbol{C}$, i.e.

$$\boldsymbol{c}_i = (c_{i1}, \ldots, c_{iM})$$

and

$$\boldsymbol{W} = (W_1, \ldots, W_M) = \left(\int_0^T S_1(t)\, X(t)\, \mathrm{d}t, \ldots, \int_0^T S_M(t)\, X(t)\, \mathrm{d}t\right)$$

is a random vector the distribution of which is independent of $i$.

Proof. Let us assume that the $i$th information symbol is transmitted. Under this condition it follows from (1) and from the definition of configuration matrix $\boldsymbol{C}$

$$\boldsymbol{Z} = \left(\int_0^T S_1(t)\,(S_i(t) + X(t))\, \mathrm{d}t, \ldots, \int_0^T S_M(t)\,(S_i(t) + X(t))\, \mathrm{d}t\right) =$$

$$= (c_{i1} + W_1, \ldots, c_{iM} + W_M) = \boldsymbol{c}_i + \boldsymbol{W}. \qquad \square$$

Measures $\mu_1, \ldots, \mu_M$ are very simple if the channel is Gaussian. We speak about a *Gaussian channel* if random variables $I(S)$, $S \in L_2$, of part (b) above are normal with the variance

$$\int_0^T S^2(t)\, \mathrm{d}t\,,$$

i.e. if the noise is white Gaussian with spectral density 1. In this case the signal power $E/T$ represents a *signal-to-noise ratio*). The following assertion holds (cf. e.g. [5]).

**Proposition 2.** If the channel is Gaussian then the random vector $\boldsymbol{W}$ of Proposition 1 has the $M$-dimensional normal distribution $N(0, \boldsymbol{C})$, where $\boldsymbol{C}$ is the configuration matrix of the signal alphabet.

**Corollary.** For every $i = 1, \ldots, M$ it holds $\mu_i = N(\boldsymbol{c}_i, \boldsymbol{C})$, where $\boldsymbol{c}_i$ is as in Proposition 1, i.e.

$$\boldsymbol{c}_i = \boldsymbol{1}_i \boldsymbol{C}$$

where all components of $\boldsymbol{1}_i$ are zero but the $i$th which is 1.

## 2. OPTIMUM DEMODULATION

In Section 1 we formulated the demodulation as a statistical decision problem with parameter and decision spaces $\{1, \ldots, M\}$ and $\{1, \ldots, M'\}$ respectively, and with a family $\{\mu_i \mid i = 1, \ldots, M\}$ of probability measures on $(\mathbb{R}^M, \mathscr{B}^M)$. This problem is defined completely after specifying a loss function

$$L(i, j)\,, \quad i = 1, \ldots, M\,, \quad j = 1, \ldots, M'$$

and a prior probability distribution $\boldsymbol{p} = (p_1, \ldots, p_M)$ on the parameter space. In this paper we consider the hard decision case where $M' = M$, and where the only natural

candidate for the loss function is

$$L(i,j) = \begin{cases} 0 & \text{if} \quad i = j \\ 1 & \text{if} \quad i \neq j \end{cases}$$

Unless otherwise explicitly stated, we restrict ourselves to the uniform prior distribution

$$\boldsymbol{p} = \boldsymbol{p}_U = \left(\frac{1}{M}, \frac{1}{M}, \ldots, \frac{1}{M}\right). \tag{2}$$

Under these assumptions with each decision function $\Delta$ we connect a *risk*

$$\mathscr{R}(\Delta) = \frac{1}{M} \sum_{i=1}^{M} \mu_i(E_i^c) = \frac{1}{M} \sum_{i=1}^{M} (1 - \mu_i(E_i))$$

where $\mathscr{E}_\Delta = (E_i = \Delta^{-1}(i) \mid i = 1, \ldots, M)$ is a measurable disjoint decomposition of the sample space $\mathbb{R}^M$. It is well known that a decision function $\Delta$ minimizes the risk (i.e. attains the so called *Bayes risk* of the problem) iff for every $i \in \{1, \ldots, M\}$ and every $z \in E_i = \Delta^{-1}(i)$

$$m_i(z) = \max_{j=1,\ldots,M} m_j(z), \tag{3}$$

where $m_j$ is the Radon-Nikodym density $\mathrm{d}\mu_j/\mathrm{d}\mu$ with respect to a $\sigma$-finite measure $\mu$ dominating the family $\{\mu_i \mid i = 1, \ldots, M\}$. A minimum risk decision function $\Delta$ (or a minimum risk measurable decomposition $\mathscr{E}$ of $\mathbb{R}^M$) is called the *optimum demodulation*.

**Proposition 3.** If $\mathscr{E} = (E_i \mid i = 1, \ldots, M)$ is an optimum demodulation then

$$\mu_i(E_i) = \max_{j=1,\ldots,M} \mu_j(E_i), \quad i = 1, \ldots, M.$$

Proof. It suffices to integrate both sides of (3) over $E_i$ with respect to the measure $\mu$ and to take into account the evident relations

$$\max_{j=1,\ldots,m} \int_{E_i} m_j(z)\, \mathrm{d}\mu(z) \leqq \int_{Ei} \max_{j=1,\ldots,m} m_j(z)\, \mathrm{d}\mu(z)$$

and

$$\mu_i(E_i) \leqq \max_{i=1,\ldots,M} \mu_j(E_i). \qquad \square$$

**Proposition 4.** Let the channel be Gaussian. Then (3) holds for $z = (z_1, \ldots, z_M) \in \in \mathbb{R}^M$ if

$$z_i = \max_{j=1,\ldots,M} z_j \tag{4}$$

If the configuration matrix $\boldsymbol{C}$ is regular then the statement above holds with "if" replaced by "iff".

Proof. (1) Let us first assume that $\boldsymbol{C}$ is regular. Choose $j \in \{1, \ldots, M\}$. By Proposition 2, the density $m_j(z)$ is a decreasing function of the quadratic form

$$(z - \boldsymbol{1}_j\boldsymbol{C})\,\boldsymbol{C}^{-1}(z - \boldsymbol{1}_j\boldsymbol{C})^{\mathrm{T}} = (z\boldsymbol{C}^{-1} - \boldsymbol{1}_j)\,(z - \boldsymbol{1}_j\boldsymbol{C})^{\mathrm{T}} =$$

$$= (zC^{-1} - I_j)(z^T - CI_j^T) = zC^{-1}z^T - zI_j^T - I_jz^T + I_jCI_j^T =$$
$$= zC^{-1}z^T - 2z_j + C_{jj} = zC^{-1}z^T - 2z_j + E .$$

Therefore (3) holds iff (4) holds.

(2) Let us now suppose that the rank of $C$ is $m < M$. Since $C$ has positive elements $E$ on the diagonal, it holds $m \geqq 1$. Further, since $C$ is symmetric, we may assume without loss of generality that it holds

$$C = \left(\begin{array}{c|c} C_1 & C_2 \\ \hline C_2^T & C_3 \end{array}\right)$$

where $C_1$ is a regular $m \times m$ matrix. Finally, it follows from Proposition 2 that there exists an $m \times (M - m)$ matrix $D$ such that the random vector $W$ defined there satisfies the relation

$$(W_{m+1}, \ldots, W_M) = (W_1, \ldots, W_m)\, D .$$

This relation can be rewritten into the form

$$W = (W_1, \ldots, W_m)\,(I_m \mid D)$$

where, here and in the sequel, $I_m$ denotes the unit $m \times m$ matrix. The relations

$$\mathsf{E}W^TW = C , \quad \mathsf{E}(W_1, \ldots, W_m)^T (W_1, \ldots, W_m) = C_1$$

imply the identity

$$C = \left(\begin{array}{c} I_m \\ \hline D^T \end{array}\right) C_1 (I_m \mid D) .$$

It follows from there

$$\left(\begin{array}{c|c} C_1 & C_2 \\ \hline C_2^T & C_3 \end{array}\right) = \left(\begin{array}{c} C_1 \\ \hline D^TC_1 \end{array}\right)(I_m \mid D)$$

$$= \left(\begin{array}{c|c} C_1 & C_1D \\ \hline D^TC_1 & D^TC_1D \end{array}\right) = \left(\begin{array}{c|c} C_1 & C_1D \\ \hline (C_1D)^T & (C_1D)^T D \end{array}\right)$$

i.e. $C_2 = C_1D$ and

$$\left(\begin{array}{c|c} C_1 & C_2 \\ \hline C_2^T & C_3 \end{array}\right) = \left(\begin{array}{c} C_1 \\ \hline C_2^T \end{array}\right)(I_m \mid D) .$$

Multipying both sides of this identity from the left by $I_j$ one obtain the relations

$$c_j = (c_{j1}, \ldots, c_{jm})\,(I_m \mid D) , \quad j = 1, \ldots, M .$$

Therefore if $z \in \mathbb{R}^m$ then there exists $j \in \{1, \ldots, M\}$ with the property

$$z - c_j = (z_1 - c_{j1}, \ldots, z_m - c_{jm})\,(I_m \mid D)$$

iff

$$z = (z_1, \ldots, z_m)\,(I_m \mid D) , \tag{5}$$

in which case all $j \in \{1, \ldots, M\}$ are possessing this property.

(3) Let the assumptions and notations of part (2) hold and let us denote by $(z)_m$ and $(c_j)_m$ the subvectors consisting of the first $m$ coordinates of $z$ and $c_j$. It follows

from the result of part (2) and from Proposition 2 that it holds

$$m_j(z) = \text{const.} \exp\{-((z)_m - (c_j)_m)\, C_1^{-1}((z)_m - (c)_m - (c_j)_m)^{\mathrm{T}}\} \tag{6}$$

for $j = 1, \ldots, M$ or $m_j(z) = 0$ for $j = 1, \ldots, M$, depending on whether $z$ satisfies (5) or not. If $z$ satisfies (5) then the quadratic form occurring in (6) equals

$$(z)_m\, C_1^{-1}(z)_m^{\mathrm{T}} - 2z_j + E$$

for every $j \in \{1, \ldots, M\}$. This fact can be proved by the method of part (1) if $j \in \in \{1, \ldots, m\}$. For $j \in \{m+1, \ldots, M\}$ it suffices to use the same method provided one takes into account the relations

$$(c_j)_m = \sum_{k=1}^{m} a_k (c_k)_m$$

and

$$z_j = \sum_{k=1}^{m} a_k z_k\,,$$

where $(a_1, \ldots, a_m)^{\mathrm{T}}$ denotes the $(j-m)$th column of the matrix $\boldsymbol{D}$ of part (2). Now we can conclude that if (4) holds then (3) holds too because either (5) is not satisfied, in which case $m_1(z) = \ldots = m_M(z) = 0$, or (5) is satisfied and $m_i(z)$ is at least as large as any quantity occurring in (6), respectively. □

Let us now return back to the general not necessarily Gaussian channel. The relation (3) represents the well-known *maximum likelihood deciston rule.* Hence the optimum demodulation is nothing but a maximum likelihood decision.

Analogically as in the statistical model with family $(\mu_i \mid i = 1, \ldots, M)$ of measures induced by the family $(\nu_i \mid i = 1, \ldots, M)$, one can consider optimum demodulation directly in the statistical model with the family $(\nu_i \mid i = 1, \ldots, M)$. To this end it suffices to consider the Radon-Nikodym densities $n_i = \mathrm{d}\nu_i/\mathrm{d}\nu$ of measures $\nu_i$ with respect to a dominating $\sigma$-finite measure $\nu$ as functions of realizations $y \in \mathbb{R}^{[0,T]}$ of the received random waveform $Y(t)$. If a measurable disjoint decomposition $\mathscr{F} = (F_i \mid i = 1, \ldots, M)$ od $\mathbb{R}^{[0,T]}$ is a maximum likelihood decision rule, i.e. if it holds for every $i = 1, \ldots, M$

$$n_i(y) = \max_{j=1,\ldots,M} n_j(y)\,, \quad y \in F_i\,,$$

then the risk of $\mathscr{F}$ is obviously the Bayes risk of the latter problem. It is known (cf. [4]), that this risk never exceeds the Bayes risk of the former problem.

**Proposition 5.** If the channel is Gaussian then the Bayes risk of the experiment $(\nu_i \mid i = 1, \ldots, M)$ is the same as the Bayes risk of the experiment $(\mu_i \mid i = 1, \ldots, M)$.

Proof. Kailath [5] has shown that there exists a function $g(y)$ on $\mathbb{R}^{[0,T]}$ such that

$$n_i(y) = g(y) \exp\{z_i\}\,, \quad i = 1, \ldots, M\,,$$

where $z_i$ is the $i$th coordinate of the statistic defined by (2). It follows from here that if $\mathscr{F} = (F_i \mid i = 1, \ldots, M)$ is a maximum likelihood decision scheme for

$(\nu_i \mid i = 1, \ldots, M)$ then there exist a decision scheme $\mathscr{E} = (E_i \mid i = 1, \ldots, M)$ for $(\mu_i \mid i = 1, \ldots, M)$ such that

$$F_i = \boldsymbol{Z}^{-1} E_i , \quad i = 1, \ldots, M .$$

Let us notice that, by Proposition 4, $\mathscr{E}$ is a maximum likelihood decision scheme for $(\mu_i \mid i = 1, \ldots, M)$. Since $\mu_i = \nu_i \boldsymbol{Z}^{-1}$, it holds

$$\frac{1}{M} \sum_{i=1}^{m} (1 - \nu_i(F_i)) = \frac{1}{M} \sum_{i=1}^{M} (1 - \mu_i(E_i))$$

i.e., the risks of both schemes are the same. □

Thus in the Gaussian channel nothing is lost by the restriction to the correlation demodulation based on the statistic (2).

The following assertion is useful in evaluating the risk of demodulation. Let us remind than a square matrix $\boldsymbol{R}$ is said orthogonal if it is regular and if its inverse $\boldsymbol{R}^{-1}$ equals $\boldsymbol{R}^{\mathrm{T}}$.

**Proposition 6.** Let $\boldsymbol{X} = (X_1, \ldots, X_M)$ be a random vector with uncorrelated standard normal components and let the channel be Gaussian. Then there exists an $M \times M$ matrix $\boldsymbol{B}$ such that the random vector of Proposition 1 satisfies the relation

$$\boldsymbol{W} = \boldsymbol{X}\boldsymbol{B} .$$

If the first $m$ eigenvalues of the positively semidefinite symmetric configuration matrix $\boldsymbol{C}$ are $\lambda_1 > 0, \ldots, \lambda_m > 0$ and the remaining eigenvalues are zero then it holds $\boldsymbol{B} = \boldsymbol{\Lambda}^{1/2}\boldsymbol{R}$, where $\boldsymbol{R}$ is an orthogonal $M \times M$ matrix which diagonalizes $\boldsymbol{C}$, i.e. where

$$\boldsymbol{R}^{\mathrm{T}}\boldsymbol{C}\boldsymbol{R} = \left(\begin{array}{ccc|c} \lambda_1 & & 0 & \\ & \ddots & & 0 \\ 0 & & \lambda_m & \\ \hline & 0 & & 0 \end{array}\right) \triangleq \boldsymbol{\Lambda} ,$$

and $\boldsymbol{\Lambda}^{1/2}$ is the usual square root of $\boldsymbol{\Lambda}$.

Proof. Let $\boldsymbol{B} = \boldsymbol{\Lambda}^{1/2}\boldsymbol{R}$ and $\boldsymbol{W} = \boldsymbol{X}\boldsymbol{B}$. Then it holds

$$\mathsf{E}\boldsymbol{W} = 0$$

and

$$\mathsf{E}\boldsymbol{W}^{\mathrm{T}}\boldsymbol{W} = \boldsymbol{B}^{\mathrm{T}}\,\mathsf{E}\boldsymbol{X}^{\mathrm{T}}\boldsymbol{X}\boldsymbol{B} = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{I}_M\boldsymbol{B} = \boldsymbol{B}^{\mathrm{T}}\boldsymbol{B} = \boldsymbol{R}^{\mathrm{T}}\boldsymbol{\Lambda}^{1/2}\boldsymbol{\Lambda}^{1/2}\boldsymbol{R} = \boldsymbol{C} .$$

The desired assertion thus follows from Proposition 2. □

**Corollary.** If the assumptions of Proposition 6 hold then the optimum demodulation is defined by a disjoint decomposition $\mathscr{D} = (D_i \mid i = 1, \ldots, M)$ of the sample space $\mathbb{R}^m$ of the subvector $(Z_1, \ldots, Z_m)$ of $\boldsymbol{Z}$ defined by (4) under the condition (5). Moreover, if

(7) $\quad p_{ij} = \mu_i(D_j \times \mathbb{R}^{M-m}) = \mathrm{Prob}\,\{(c_i)_m + (W_1, \ldots, W_m) \in D_j\} , \quad i, j = 1, \ldots, M ,$

then

$$\mathscr{R} = \frac{1}{M} \sum_{i=1}^{M} \sum_{j \neq i} p_{ij} = \frac{1}{M} \sum_{i=1}^{M} (1 - p_{ii}) \tag{8}$$

is the risk of optimum demodulation.

Proof. Analogically as in part (2) of the proof of Proposition 4, we find that it holds

$$\boldsymbol{Z} = (Z_1, \ldots, Z_m)\,(\boldsymbol{I}_m \mid \boldsymbol{D}) \quad \text{(cf. (5))}\,.$$

The rest is clear from here, from Proposition 4, and from the definition of risk. □

## 3. EXAMPLES

**Example 1.** Let us consider the signal alphabet $\mathscr{S} = (S_1(t), S_2(t))$ where

$$S_1(t) = \sqrt{\left(\frac{2E}{T}\right)} \sin \frac{2\pi k t}{T}\,, \quad S_2(t) = -S_1(t)\,,$$

where $k$ is a natural number. The configuration matrix is in this case given by

$$C = \begin{pmatrix} E & -E \\ -E & E \end{pmatrix}. \tag{9}$$

For a received random waveform $(Y(t) \mid 0 \leqq t \leqq T)$ we consider the statistic

$$\boldsymbol{Z} = (Z_1, Z_2) = (Z_1, -Z_1)$$

where

$$Z_1 = \sqrt{\left(\frac{2E}{T}\right)} \int_0^T Y(t) \sin \frac{2\pi k t}{T}\, \mathrm{d}t\,.$$

It holds

$$Z_1 = \begin{cases} E + W_1 & \text{if} \quad i = 1 \\ -E - W_1 & \text{if} \quad i = 2\,, \end{cases} \tag{10}$$

where

$$W_1 = \sqrt{\left(\frac{2E}{T}\right)} \int_0^T X(t) \sin \frac{2\pi k t}{T}\, \mathrm{d}t\,.$$

Let us now assume that the channel is Gaussian. By Proposition 2 it holds

$$W_1 = N(0, E)\,.$$

Further, by Proposition 4, the optimum demodulation of the information symbol $i = 1$ is defined by the condition $Z_1 \geqq Z_2$, i.e. by $Z_1 \geqq -Z_1$ or, equivalently, by $Z_1 \geqq 0$. Analogically, the optimum demodulation of the information symbol $i = 2$ is defined by the condition $Z_1 < 0$. Thus, in accordance with Corollary to Proposition 6, the optimum demodulation is defined simply by the decomposition $\mathscr{D} = (D_1 = [0, \infty), D_2 = (-\infty, 0))$ of the sample space $\mathbb{R}$ of random variable $Z_1$. Let

us denote by $p$ the common value of the probability

$$p_{12} = \text{Prob}\{E + W_1 \in D_2\} = \text{Prob}\{-E - W_1 \in D_1\} = p_{21}.$$

It follows from the formula for $W_1$ above that

$$p = \frac{1}{\sqrt{(2\pi E)}} \int_{-\infty}^{0} \exp\left\{-\frac{(z_1 - E)^2}{2E}\right\} dz_1 = \frac{1}{\sqrt{(2\pi)}} \int_{-\infty}^{-\sqrt{E}} \exp\left\{-\frac{x^2}{2}\right\} dx = \Phi(-\sqrt{E}).$$

By (8), the risk connected with the optimum demodulation satisfies the relation

$$\mathscr{R} = p.$$

This risk, as a function of the signal energy $E$ (or of the signal-to-noise ratio $E/T$ in decibels, for $T = 0{\cdot}005$), is shown in Figure 1.

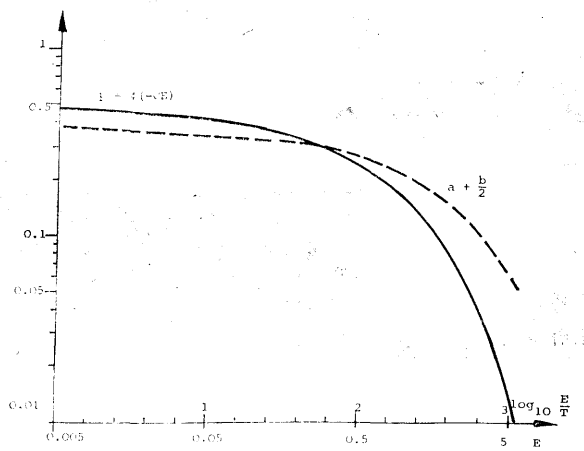



**Fig. 1.** $T = 0{\cdot}005$ sec (for $a + b/2$ cf. Fig. 3).

**Example 2.** Let us consider the signal alphabet $\mathscr{S}$ for $M = 4$ with

$$S_1(t) = \sqrt{\left(\frac{2E}{T}\right)} \sin\frac{2\pi kt}{T}, \quad S_2(t) = \sqrt{\left(\frac{2E}{T}\right)} \cos\frac{2\pi kt}{T},$$

$$S_3(t) = -S_1(t), \quad S_4(t) = -S_2(t),$$

where $k$ is a natural number. The configuration matrix of this alphabet is

$$C = \begin{pmatrix} E & 0 & -E & 0 \\ 0 & E & 0 & -E \\ -E & 0 & E & 0 \\ 0 & -E & 0 & E \end{pmatrix}. \tag{11}$$

Let us note that in this as well as in the previous example the configuration matrix is *circulant*, i.e. its rows are cyclic shifts of the first row. A general theory of signal alphabets with circulant configuration matrices can be found in [2].

For the received random waveform $(Y(t) \mid 0 \leqq t \leqq T)$ we consider the statistic

$$\boldsymbol{Z} = (Z_1, Z_2, Z_3, Z_4) = (Z_1, Z_2, -Z_1, -Z_2)$$

where

$$Z_1 = \sqrt{\left(\frac{2E}{T}\right)} \int_0^T Y(t) \sin \frac{2\pi kt}{T} \, \mathrm{d}t \,,$$

$$Z_2 = \sqrt{\left(\frac{2E}{T}\right)} \int_0^T Y(t) \cos \frac{2\pi kt}{T} \, \mathrm{d}t \,.$$

It follows from Proposition 1

$$(Z_1, Z_2) = (W_1, W_2) + \begin{cases} (E, 0) & \text{if } i = 1 \\ (0, E) & \text{if } i = 2 \\ (-E, 0) & \text{if } i = 3 \\ (0, -E) & \text{if } i = 4 \end{cases} \tag{12}$$

where

$$(W_1, W_2) = \sqrt{\left(\frac{2E}{T}\right)} \left( \int_0^T X(t) \sin \frac{2\pi kt}{T} \, \mathrm{d}t, \int_0^T X(t) \cos \frac{2\pi kt}{T} \, \mathrm{d}t \right).$$

Let us assume that the channel is Gaussian. In this case it follows from Proposition 2

$$(W_1, W_2) = N\left((0, 0), \begin{pmatrix} E, & 0 \\ 0, & E \end{pmatrix}\right).$$

This conclusion follows also from Proposition 6. Indeed, the assumptions of Proposition 6 hold for $m = 2, \lambda_1 = \lambda_2 = 2E$, and

$$\boldsymbol{R} = \begin{pmatrix} \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} & 0 \\ 0 & \frac{1}{\sqrt{2}} & 0 & -\frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} & 0 \\ 0 & -\frac{1}{\sqrt{2}} & 0 & \frac{1}{\sqrt{2}} \end{pmatrix}.$$

Therefore it follows from Proposition 6 that

$$(W_1, W_2, W_3, W_4) = (X_1, X_2, X_3, X_4)\boldsymbol{B}$$

where

$$\boldsymbol{B} = \boldsymbol{\Lambda}^{1/2}\boldsymbol{R} = \begin{pmatrix} \sqrt{E} & 0 & -\sqrt{E} & 0 \\ 0 & -\sqrt{E} & 0 & \sqrt{E} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

and $X_k$ are uncorrelated standard normal random variables. Therefore

$$(W_1, W_2) = \sqrt{E}(X_1, X_2), \quad (W_3, W_4) = -(W_1, W_2) \,.$$

Let us now evaluate the optimum demodulation under the assumption that the channel is Gaussian. It follows from what has been said above and from Corollary to Proposition 6 that this demodulation is given by the decomposition $\mathscr{S} = (D_1, D_2, D_3, D_4)$ of the sample space $\mathbb{R}^2$ of the random vector $(Z_1, Z_2)$ defined by

$$D_1 = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_1 \geqq \max\{z_2, -z_1, -z_2\}\} = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_1 \geqq |z_2|\},$$
$$D_2 = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_2 > \max\{z_1, -z_1, -z_2\}\} = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_2 > |z_1|\},$$
$$D_3 = \{(z_1, z_2) \in \mathbb{R}^2 \mid -z_1 \geqq \max\{z_1, z_2, -z_2\}\} = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_1 \leqq -|z_2|\},$$
$$D_4 = \{(z_1, z_2) \in \mathbb{R}^2 \mid -z_2 > \max\{z_1, z_2, -z_1\}\} = \{(z_1, z_2) \in \mathbb{R}^2 \mid z_2 < -|z_1|\}.$$

This decomposition is disjoint provided the point $(0, 0)$ is subtracted either from the set $D_1$ or from the set $D_3$. The sets $D_1, \ldots, D_4$ are illustrated in Figure 2.

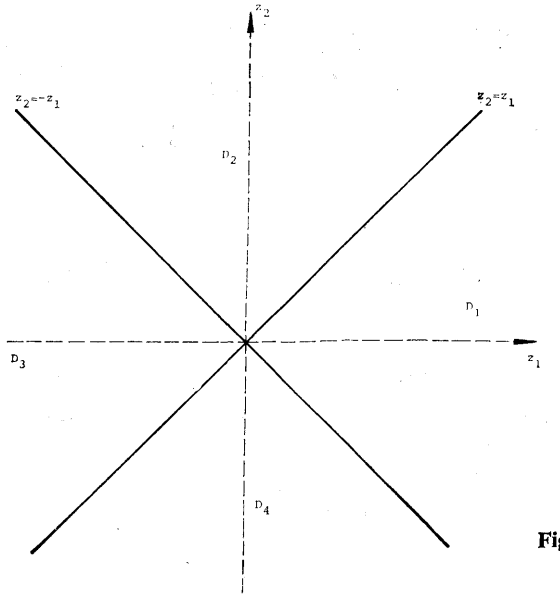



**Fig. 2.**

With the help of this illustration it follows from (12) that

$$\begin{pmatrix} p_{11} & p_{12} & p_{13} & p_{14} \\ p_{21} & p_{22} & p_{23} & p_{24} \\ p_{31} & p_{32} & p_{33} & p_{34} \\ p_{41} & p_{42} & p_{43} & p_{44} \end{pmatrix} = \begin{pmatrix} c & a & b & a \\ a & c & a & b \\ b & a & c & a \\ a & b & a & c \end{pmatrix}.$$

where

$$a = \text{Prob}\{(E, 0) + (W_1, W_2) \in D_4\} = \text{Prob}\{(E, 0) + (W_1, W_2) \in D_2\} =$$
$$= [1 - \text{Prob}\{(E, 0) + (W_1, W_2) \in D_1 \cup D_3\}] =$$
$$= \frac{1}{2}\left[1 - \frac{1}{2\pi E}\int_{D_1 \cup D_3} \exp\left\{-\frac{(z_1 - E)^2}{2E} - \frac{z_2^2}{2E}\right\} dz_1\, dz_2\right] =$$
$$= 1 - \frac{1}{\sqrt{(2\pi)}}\int_{-\infty}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} \Phi(|x + \sqrt{E}|)\, dx,$$

$$b = \text{Prob}\{E, 0) + (W_1, W_2) \in D_3\} = \text{Prob}\{(E, 0) + (W_1, W_2) \in D_2 \cup D_3\} - a =$$

$$= 1 - \frac{1}{\sqrt{(2\pi)}} \int_{-\infty}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} \Phi(x + \sqrt{E})\, dx - a =$$

$$= \frac{1}{\sqrt{(2\pi)}} \int_{\sqrt{E}}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} [2\Phi(x - \sqrt{E}) - 1]\, dx\,,$$

and

$$c = 1 - 2a - b\,.$$

The optimum demodulation risk, given by

$$\mathscr{R} = 1 - c = 2a + b\,,$$

represents the probability of error per one information symbol. Since there are 4 information symbols, the *bit error rate* $p = \mathscr{R}/2$ satisfies the relation*)

$$p = a + \tfrac{1}{2}b\,.$$

The values of $a$, $b$, $\mathscr{R}$ as functions of $E > 0$ are shown in Figure 3. The values of $a + \frac{1}{2}b$ are represented by the interrupted line in Figure 1. It follows from Figure 1 that for the signal energies $E \geqq 0{\cdot}315$ (i.e. for signal-to-noise ratios above 1·8 decibels when $T = 0{\cdot}005$ sec) the coding of bits by the signal alphabet of Example 1 is better than the coding of dibits by the signal alphabet of Example 2. For the signal energies below that level the converse is true (unsignificant in view of the footnote).

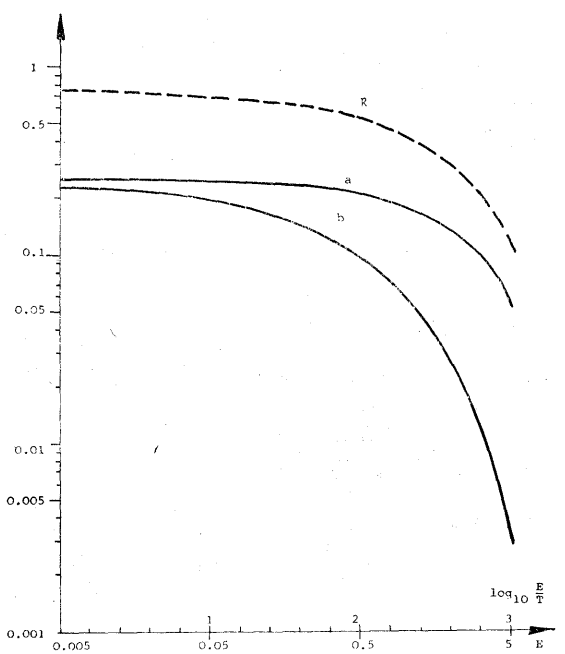



**Fig. 3.** $T = 0{\cdot}005$ sec.

*) Exact relation between the bit error rate $p$ and the symbol risk $\mathscr{R}$ for $M > 1$ is given by $(1 - p)^{\log_2 M} = 1 - \mathscr{R}$. Our simplifie approach is justified for $p < 0{,}2$.

**Example 3.** Let $\mathscr{S}$ consists of orthogonal signals i.e. let

$$C = \begin{pmatrix} E & & 0 \\ & E & \\ & \ddots & \ddots \\ 0 & & E \end{pmatrix}. \tag{13}$$

In this case, under the condition that the $i$th signal is transmitted, the statistic (1) satisfies the relation

$$Z = EI_i + W \tag{14}$$

where $W$ is defined by Proposion 1.

Let the channel be Gaussian. Then it follows from Proposition 2 that $W$ consists of $M$ uncorrelated normal random variables, each distributed by $N(0, E)$. Since the matrix C is regular, the optimum demodulation $\mathscr{E} = (E_i \mid i = 1, \ldots, M)$ is a decomposition of $\mathbb{R}^M$ defined simply by (4). It follows from a symmetry in (4) and (14)

$$\begin{pmatrix} p_{11} & \cdots & p_{1M} \\ \cdots & \cdots & \cdots \\ p_{M1} & \cdots & p_{MM} \end{pmatrix} = \begin{pmatrix} 1-p & \frac{p}{M-1} & \cdots & \frac{p}{M-1} \\ \frac{p}{M-1} & 1-p & \cdots & \frac{p}{M-1} \\ \cdots & \cdots & \cdots & \cdots \\ \frac{p}{M-1} & \frac{p}{M-1} & \cdots & 1-p \end{pmatrix}$$

where, by (7),

$$1 - p = \operatorname{Prob}\{(E, 0, \ldots, 0) + W \in E_1\} = \operatorname{Prob} \bigcap_{j=2}^{n} \{E + W_1 > W_j\} =$$

$$= \frac{1}{\sqrt{(2\pi E)}} \int_{-\infty}^{\infty} \exp\left\{-\frac{w_1^2}{2E}\right\} \operatorname{Prob} \bigcap_{j=2}^{M} \{E + w_1 > W_j\}\, dw_1 =$$

$$= \frac{1}{\sqrt{(2\pi E)}} \int_{-\infty}^{\infty} \exp\left\{-\frac{w_1^2}{2E}\right\} \Phi\left(\frac{E + w_1}{\sqrt{E}}\right)^{M-1} dw_1 =$$

$$= \frac{1}{\sqrt{(2\pi)}} \int_{-\infty}^{\infty} \exp\left\{-\frac{x^2}{2}\right\} \Phi(x + \sqrt{E})^{M-1}\, dx =$$

$$= 1 - \frac{M-1}{\sqrt{(2\pi)}} \int_{-\infty}^{\infty} \Phi(x)\, \Phi(x + \sqrt{E})^{M-2} \exp\left\{-\frac{(x + \sqrt{E})^2}{2}\right\} dx .$$

It follows from here

$$p = \frac{M-1}{\sqrt{(2\pi)}} \int_{-\infty}^{\infty} \Phi(x - \sqrt{E})\, \Phi(x)^{M-2} \exp\left\{-\frac{x^2}{2}\right\} dx . \tag{15}$$

Further, by (8) the risk of the optimum demodulation satisfies the relation

$$\mathscr{R} = p .$$

The quantity

$$\frac{\mathscr{R}}{\log_2 M} = \frac{p}{\log_2 M}$$

characterizes the demodulation bit *error rate* (cf. footnote on p. 186). The risk, as a function of the signal energy $E > 0$, is shown for $M = 32$ and $M = 256$ in Fig. 1 on p. 568 of Gallager [3].

Taking into account the inequality $\Phi(x - \sqrt{E}) \leqq \Phi(x)$ in (15) we see that it holds

$$p \leqq \frac{M-1}{\sqrt{(2\pi)}} \int_{-\infty}^{\infty} \Phi(x)^{M-1} \left\{-\frac{x^2}{2}\right\} dx = (M-1) \int_0^1 x^{M-1}\, dx = \frac{M-1}{M}.$$

Therefore it holds in the matrix considered above

$$1 - p \geqq \frac{p}{M-1},$$

which is the property required by Proposition 3.

## 4. OPTIMUM SIGNAL ALPHABETS

In Example 2 we have seen preferences between the two-signal alphabet

$$\mathscr{S}_1 = \left\{\sqrt{\left(\frac{2E}{T}\right)} \sin\frac{2\pi kt}{T},\quad -\sqrt{\left(\frac{2E}{T}\right)} \sin\frac{2\pi kt}{T}\right\}$$

and the four-signal alphabet

$$\mathscr{S}_2 = \mathscr{S}_1 \cup \left\{\sqrt{\left(\frac{2E}{T}\right)} \cos\frac{2\pi kt}{T},\quad -\sqrt{\left(\frac{2E}{T}\right)} \cos\frac{2\pi kt}{T}\right\}$$

based on the value of the corresponding bit error rates

$$\frac{\mathscr{R}_2}{\log_2 2} = \mathscr{R}_1 \quad \text{and} \quad \frac{\mathscr{R}_2}{\log_2 4} = \frac{\mathscr{R}_2}{2}.$$

We have seen from Figure 1 that $\mathscr{S}_2$ is preferable when $E > 0{\cdot}315$ (significant case) and $\mathscr{S}_1$ is preferable when $E < 0{\cdot}315$ (unsignificant case). In the significant case the bit error probability of the alphabet $\mathscr{S}_1$ is below that of alphabet $\mathscr{S}_2$. This is quite natural because the bit transmission rate of alphabet $\mathscr{S}_2$ is twice greater than that of alphabet $\mathscr{S}_1$: a greater transmission rate leads to a greater error rate. Thus, having given a bit error rate maximum level, we may switch from the alphabet $\mathscr{S}_1$ to $\mathscr{S}_2$ only if the signal-to-noise ratio is good enough. Of course, the trade-off between the error and transmission rates makes the comparison of alphabets with different numbers $M$ of signals very complicated.

*In order to avoid these complications, we shall look more deeply at preferences between different signal alphabets of the same cardinality M.*

In Gaussian channels, where the observed statistics $\boldsymbol{Z}$ are completely determined

by the configuration matrices (cf. Propositions 1 and 2), we shall in fact compare different $M \times M$ configuration matrices. In general, our comparison is based on the matrix

$$\boldsymbol{P} = \begin{pmatrix} \boldsymbol{p}_1 \\ \vdots \\ \boldsymbol{p}_M \end{pmatrix} = \begin{pmatrix} p_{11} & \cdots & p_{1M} \\ \cdots & \cdots & \cdots \\ p_{M1} & \cdots & p_{MM} \end{pmatrix}$$

of *modulation transition probabilities* defined in general by an optimum demodulation $\mathscr{E} = (E_i \mid i = 1, \ldots, M)$, corresponding to an alphabet $\mathscr{S}$ and to a channel, by means of the formula

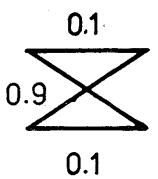
$$p_{ij} = \mu_i(E_j), \quad i, j = 1, \ldots, M .$$

If the channel is Gaussian then these probabilities are defined by (7).

The matrix $\boldsymbol{P}$ differs from the matrix of channel transition probabilities, which is common in discrete information theory, in that it possesses the property

$$p_{ii} = \max_{j=1,\ldots,M} p_{ij}, \quad i = 1, \ldots, M \tag{16}$$

resulting from Proposition 3. Thus, for example, the binary symmetric channel




seriously considered by the discrete information theory is excluded from the point of view of modulation. In general, (16) implies that the Bayes risk $\mathscr{R}$ of Section 2 coincides with the minimum average error probability

$$\mathrm{e}(\boldsymbol{P}) = \min_{\boldsymbol{T}} \frac{1}{M} \sum_{j=1}^{M} \sum_{i \neq \boldsymbol{T}(j)} p_{ij}$$

considered in discrete information theory, where the minimization extends over all mappings $\boldsymbol{T}$: $\{1, \ldots, M\} \to \{1, \ldots, M\}$. Indeed, under (16) the minimum is attained at the identity mapping $\boldsymbol{T}$ and

$$e(\boldsymbol{P}) = \frac{1}{M} \sum_{i=1}^{M} (1 - p_{ii}) \quad \text{(cf. Sec. 2, in particular (8))} . \tag{17}$$

Thus the Bayes risk $\mathscr{R}$ of Section 2, or equivalently the *error probability* $e(\boldsymbol{P})$ defined by (17), is a natural criterion of quality of a signal alphabet $\mathscr{S}$ for a channel considered in Section 1. Since the alphabet size $M$ is assumed to be fixed, no norming to the bit error rate is necessary,

There are however other possible criteria known from information theory. We shall present at least the best known of them.

We shall consider stochastic vectors $\boldsymbol{p} = (p_1, \ldots, p_M)$ from the well known simplex

$\mathbb{P} \subset \mathbb{R}^M$. By $p$, with indices or not, we denote a real number from the interval $[0, 1]$, by $p\boldsymbol{p}$ we denote the usual multiplication of a vector $\boldsymbol{p} \in \mathbb{R}^M$ and $\boldsymbol{p} + \tilde{\boldsymbol{p}}$ denotes the usual sum of vectors in $\mathbb{R}^M$.

Let us consider the *entropy*

$$H(\boldsymbol{p}) = -\sum_{i=1}^{M} p_i \log p_i\,, \quad \boldsymbol{p} = (p_1, \ldots, p_M) \in \mathbb{P}\,,$$

where, here and in the sequel, the unspecified base of logarithm is assumed to be 2 and $0 \log 0$ is assumed to be 0. Instead of $H(p, 1-p)$ we use the symbol $h(p)$ commonly used to denote the entropy of dichotomy, i.e.

$$h(p) = -p \log p - (1-p) \log (1-p)\,.$$

Each matrix $\boldsymbol{P}$ of modulation transition probabilities will be termed simply a *channel*. If $\boldsymbol{p} = (p_1, \ldots, p_M) \in \mathbb{P}$ is a stochastic input of a channel $\boldsymbol{P} = (\boldsymbol{p}_1, \ldots, \boldsymbol{p}_M)^{\mathrm{T}}$ then the *information* at the output concerning the input is defined as the difference between the entropy of unconditional stochastic output

$$\sum_{i=1}^{M} p_i \boldsymbol{p}_i$$

and of the average conditional entropy, i.e.

$$I(\boldsymbol{p}, \boldsymbol{P}) = H\Big(\sum_{i=1}^{M} p_i \boldsymbol{p}_i\Big) - \sum_{i=1}^{M} p_i H(\boldsymbol{p}_i)\,.$$

The information $I(\boldsymbol{p}, \boldsymbol{P})$ is continuous in variable $\boldsymbol{p}$ from the compact set $\mathbb{P}$. The maximum information

$$C(\boldsymbol{P}) = \max_{\boldsymbol{p}} I(\boldsymbol{p}, \boldsymbol{P})\,, \quad \text{where} \quad \boldsymbol{p} \in \mathbb{P}\,,$$

is called the *capacity* of channel $\boldsymbol{P}$. The capacity is a well known performance index for channels when coding is used. It is the upper bound of transmission rates of block codes for which the probability of error can be made arbitrarily small.

The *cutoff rate* of channel $\boldsymbol{P}$ is defined by

$$R(\boldsymbol{P}) = -\log \Big[\min_{\boldsymbol{p}} \sum_{j=1}^{M} \Big(\sum_{i=1}^{M} p_j p_{ij}^{1/2}\Big)^2\Big]\,, \tag{20}$$

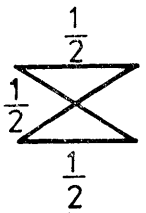
where the min is over all $\boldsymbol{p} \in \mathbb{P}$. This is an important characteristic of the channel from the point of view of coding. Indeed, with convolutional coding and sequential decoding, the cutoff rate is the upper bound of code rates for which the average per bit computation is finite (cf. [6]).

An $M \times M$ matrix, is said permutational if it is doubly stochastic and its elements are 0's and 1's. If $i_1, \ldots, i_M$ are positions of 1's in the rows $1, \ldots, M$ then $(i_1, \ldots, i_M)$ is the permutation of $(1, \ldots, M)$ represented by this matrix. The unit matrix $\boldsymbol{I}_M$ represents the identical permutation.

A channel $\boldsymbol{P}$ is said *permutational* if

$$\boldsymbol{P} = \tfrac{1}{2}(\boldsymbol{I}_M + \boldsymbol{P}_M)$$

where $\boldsymbol{P}_M$ is a permutational matrix with 0's on the diagonal. This channel can equivalently be defined by the property that in each row and each column there are just two nonzero elements which are $\frac{1}{2}$ and one of these elements is diagonal. Permutational channels will be denoted by $\boldsymbol{P}^*$ and their row vectors by $\boldsymbol{p}_i^*$. These channels represent a generalization of binary symmetric channels




to the case $M \geqq 2$. We present in Figure 4 two examples for $M = 4$.

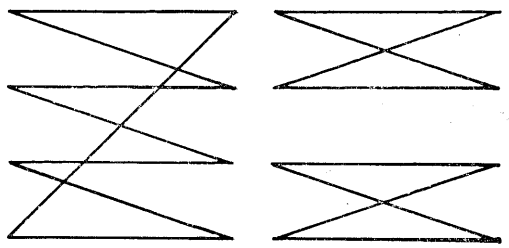
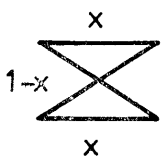


**Fig. 4.** All transitions are from left to right and their probabilities are $\frac{1}{2}$.

A channel $\boldsymbol{P}$ is said a *symmetric* with a parameter $0 \leqq x \leqq (M-1)/M$ if

$$p_{ij} = \begin{cases} 1 - x & \text{if } j = i, \\ \dfrac{x}{M-1} & \text{if } j \neq i \end{cases} \qquad i = 1, \ldots, M.$$

We restrict ourselves to symmetric channels with parameter $0 \leqq x < \frac{1}{2}$ and denote these channels by $\boldsymbol{P}^x$. By $\boldsymbol{p}_i^x$ we denote the row vectors of the matrix $\boldsymbol{P}^x$. This channel is a common generalization of the binary symmetric channel




to $M > 2$.

A channel $\boldsymbol{P}$ is said realizable by a demodulation if for every $\varepsilon > 0$ there exists a signal alphabet and a channel such that the vectors $(\mu_i(E_1), \ldots, \mu_i(E_M))$ corresponding to an optimum demodulation $(E_1, \ldots, E_M)$ differ from the row vectors $\boldsymbol{p}_i$ of $\boldsymbol{P}$ in the norm of $\mathbb{R}^M$ at most $\varepsilon$, for $i = 1, \ldots, M$. Since $e(\boldsymbol{P})$, $I(\boldsymbol{p}, \boldsymbol{P})$ and $C(\boldsymbol{P})$ are continuous functions of row vectors $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_M \in \mathbb{P}$, they can be arbitrarily closely approxim-

ated in the realizable case by channels actually resulting from a demodulation procedure.

**Proposition 7.** All symmetric channels and at least one permutation channel for $M = 4$ are realizable.

Proof. The realizability of symmetric channels follows from Example 3. We shall prove the second assertion. Let us consider a signal alphabet with the configuration matrix

$$\boldsymbol{C} = \begin{pmatrix} E & -E & E & -E \\ -E & E & -E & E \\ E & -E & E & -E \\ -E & E & -E & E \end{pmatrix}.$$

As proved by Slepian [7], for every symmetric positively semidefinite configuration matrix there exists a signal alphabet. For the present matrix this alphabet may be e.g.

$$\mathscr{S} = \left(S_1(t) = \sqrt{\left(\frac{2E}{T}\right)} \sin \frac{2\pi k t}{T},\quad S_2(t) = -S_1(t),\quad S_3(t) = S_1(t),\quad S_4(t) = S_2(t)\right).$$

Let us consider the Gaussian channel. It follows from Proportions 1 and 2 that in this case

$$\mu_1 = \mu_3 \quad \text{and} \quad \mu_2 = \mu_4 .$$

For the generalized information symbols "1 or 3" and "2 or 4" the optimum demodulation is as in Example 1, with probability of error $p = \Phi(-\sqrt{E})$. The optimum choice of 1 and 3 or 2 and 4 within the generalized symbols may be random with probability $\frac{1}{2}$. Thus

$$\mu_1(E_1) = \mu_1(E_3) = \tfrac{1}{2}(1 - \Phi(-\sqrt{E})),$$
$$\mu_1(E_2) = \mu_1(E_4) = \tfrac{1}{2}\Phi(-\sqrt{E}),$$

and analogically for $i = 2, 3, 4$. These probabilities approximate for sufficiently large $E$ the transition probabilities presented in the right-hand example for Figure 4. □

**Proposition 8.** For a permutational channel $\boldsymbol{P}^*$ it holds

$$e(\boldsymbol{P}^*) = \tfrac{1}{2},$$
$$I(\boldsymbol{p}_U, \boldsymbol{P}^*) = C(\boldsymbol{P}^*) = R(\boldsymbol{P}^*) = \log M - 1 .$$

Proof. Since $1 - p^*_{ii} = \frac{1}{2}$, the formula for $e(\boldsymbol{P}^*)$ is clear from (17). Further

$$\frac{1}{M} \sum_{i=1}^{M} \boldsymbol{p}_i^* = \boldsymbol{p}_U \quad \text{(cf. (2))}$$

so that

$$H\left(\frac{1}{M} \sum_{i=1}^{M} \boldsymbol{p}_i^*\right) = \log M .$$

The formula for $I(\boldsymbol{p}_U, \boldsymbol{P}^*)$ follows from here, from (18) and from the obvious relation

$$H(\boldsymbol{p}_i) = \log 2 .$$

We also see from here that, for every $\boldsymbol{p} \in \mathbb{P}$,

$$I(\boldsymbol{p}, \boldsymbol{P}^*) = H(\sum_{i=1}^{M} p_i p_i^*) - \log 2\,,$$

where the sum equals

$$(\tfrac{1}{2}(\boldsymbol{p}_1 + \boldsymbol{p}_{i_1}), \ldots, \tfrac{1}{2}(\boldsymbol{p}_M + \boldsymbol{p}_{i_M}))$$

and $(i_1, \ldots, i_M)$ is the permutation from the definition of $\boldsymbol{P}^*$. The entropy of this stochastic vector is maximum when $\boldsymbol{p} = \boldsymbol{p}_U$. Therefore it follows from (19) that $C(\boldsymbol{P}^*) = I(\boldsymbol{p}_U, \boldsymbol{P}^*)$. Finally, for every $\boldsymbol{p} \in \mathbb{P}$,

$$\sum_{i=1}^{M} p_j (p_{ij}^*)^{1/2} = \frac{1}{\sqrt{2}} (p_j + \boldsymbol{p}_{k_j})$$

where $i_k = j$ for $k = k_j$. Therefore

$$R(\boldsymbol{P}^*) = -\log [\min_{\boldsymbol{p}} \tfrac{1}{2} \sum_{j=1}^{M} (p_j + \boldsymbol{p}_{k_j})^2]\,,$$

where the min is over all $\boldsymbol{p} \in \mathbb{P}$. The sum is minimized if $\boldsymbol{p} = \boldsymbol{p}_U$ and its minimum value is $4/M$. Thus the formula for $R(\boldsymbol{P}^*)$ holds. □

**Proposition 9.** For a symmetric channel $\boldsymbol{P}^x$ it holds

$$e(\boldsymbol{P}^x) = x\,,$$

$$I(\boldsymbol{p}_U, \boldsymbol{P}^x) = C(\boldsymbol{P}^x) = \log M - h(x) - x \log (M - 1)$$

and

$$R(\boldsymbol{P}^x) = \log \frac{M}{[\sqrt{(1 - x)} + \sqrt{(x(M - 1))}]^2}\,.$$

Proof. The formula for $e(\boldsymbol{P}^x)$ is clear from the equality $1 - p_{ii}^x = x$. Further

$$\frac{1}{M} \sum_{i=1}^{M} \boldsymbol{p}_i^x = \boldsymbol{p}_U$$

and

$$H(\boldsymbol{p}_i^x) = h(x) + \log (M - 1)$$

so that the formula for $I(\boldsymbol{p}_U, \boldsymbol{P}^x)$ is clear from (18). The capacity is equal to this information for the same reason as in the previous proof. It remains to evaluate the cutoff rate. It holds for every $\boldsymbol{p} \in \mathbb{P}$

$$\sum_{i=1}^{M} p_j (p_{ij}^x)^{1/2} = p_j \left( \sqrt{(1 - x)} + (M - 1) \sqrt{\left( \frac{x}{M - 1} \right)} \right).$$

Since

$$\min_{\boldsymbol{p}} [\sqrt{(1 - x)} + \sqrt{((M - 1)\, x)}]^2 \sum_{j=1}^{M} p_j^2 = \frac{1}{M} [\sqrt{(1 - x)} + \sqrt{((M - 1)\, x)}]^2\,,$$

where the min is over all $\boldsymbol{p} \in \mathbb{P}$, the desired formula follows from (20). □

Using formulas of Propositions 8 and 9, the quantities $e(\boldsymbol{P})$, $I(\boldsymbol{p}_U, \boldsymbol{P})$, $C(\boldsymbol{P})$ and $R(\boldsymbol{P})$ for $\boldsymbol{P} \in \{\boldsymbol{P}^*, \boldsymbol{P}^x\}$ have been evaluated in Figure 5.

Any of the functions $e(\boldsymbol{P}), I(\boldsymbol{p}_U, \boldsymbol{P}), C(\boldsymbol{P}), R(\boldsymbol{P})$ can be used as a criterion of choice

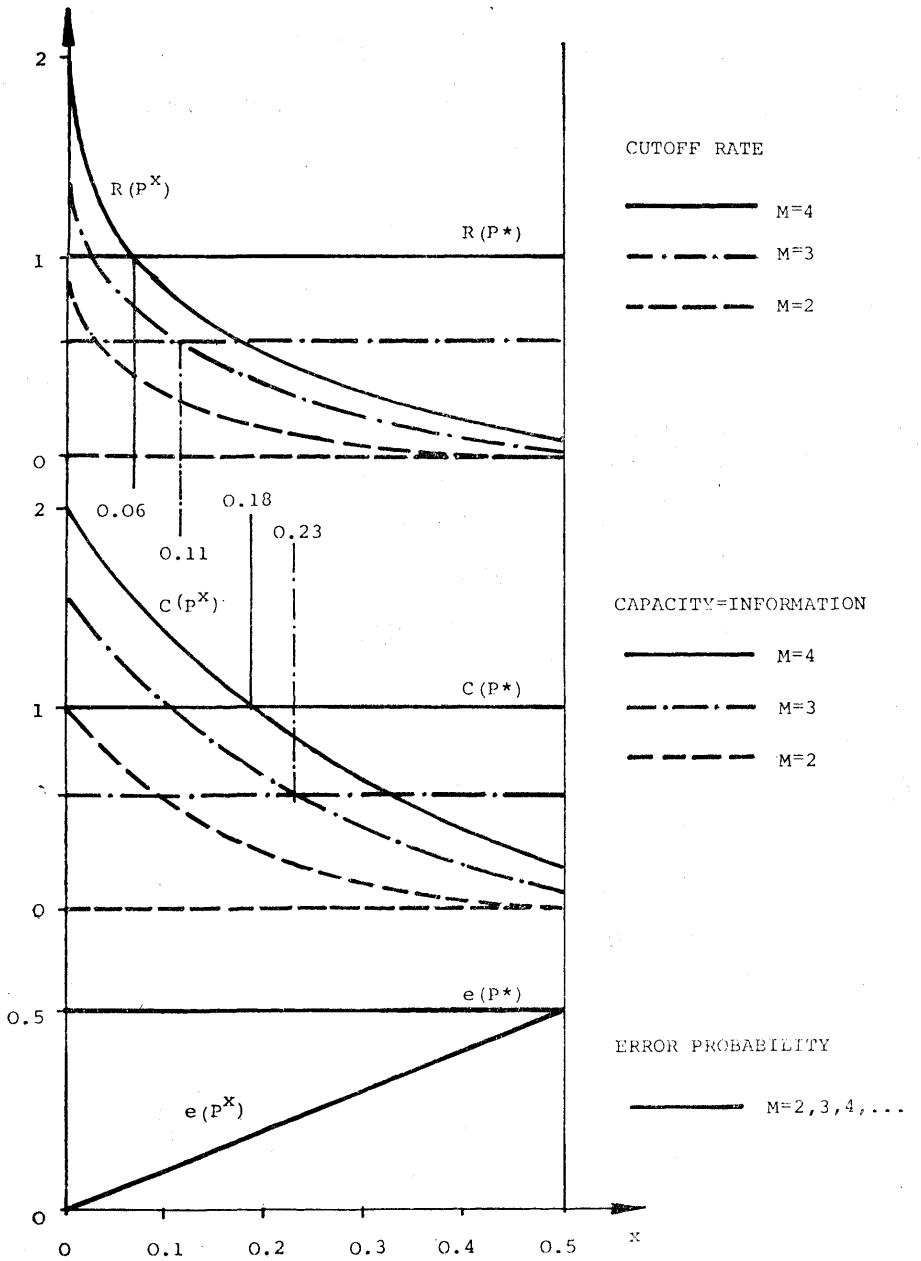



**Fig. 5.**

of an optimum signal alphabet. The error probability $e(\boldsymbol{P})$ is minimized and the remaining functions are maximized. Smaller probability of error usually means greater information, capacity and cutoff rate. The curves of Figure 5 are interesting in that they offer efficient counterexamples to this rule. At first sight it is clear that, when passing from $\boldsymbol{P}^*$ to $\boldsymbol{P}^x$, one may quite essentially decrease the probability of error and, at the same time, quite essentially decrease the capacity (information) and cutoff rate. The existence of such paradoxes was admitted, but not explicitly documented, in the literature. The quantitative extent of paradoxes offered by the channels $\boldsymbol{P}^*$ and $\boldsymbol{P}^x$ is quite surprising. It is studied in detail in the next section.

## 5. PARADOXES IN SIGNAL ALPHABETS

By Proposition 7, all symmetric channels $\boldsymbol{P}^x$ are realizable by certain signal alphabets in Gaussian channels. The same holds also for permutation channels (Proposition 7 is in this respect restricted to $M = 4$ but this alphabet size suffices to realize the paradoxes considered below not only qualitatively but, more or less, also quantitatively). Therefore the paradoxical properties of channels $\boldsymbol{P}^*$ and $\boldsymbol{P}^x$ considered in this section are in fact paradoxical properties of certain concrete alphabets.

To be explicite in this important point, let us consider an example of size $M = 4$ alphabets

$$\mathscr{S}_1 = (c_1 S(t; m), c_1 S(t; m), -c_1 S(t; m), -c_1 S(t; m))$$

and

$$\mathscr{S}_2 = (c_2 S(t; m), c_2 C(t; m), c_2 S(t; n), c_2 C(t; n)), \quad m \neq n,$$

where $S(t; k)$ denotes the sine and $C(t; k)$ the cosine of the argument

$$\frac{2\pi k t}{T}.$$

Let the channel be Gaussian. Then the matrix of modulation transition probabilities of $\mathscr{S}_i$ is $\boldsymbol{P}^x$ where (cf. Example 3, in particular (10))

$$x = \frac{3}{\sqrt{(2\pi)}} \int_{-\infty}^{\infty} \Phi(u - c_1 \sqrt{T})\, \Phi(u)^2 \exp\{-\tfrac{1}{2}u^2\}\, du .$$

We see from here that all $0 < x < \frac{1}{2}$, which we are interested in from the last section

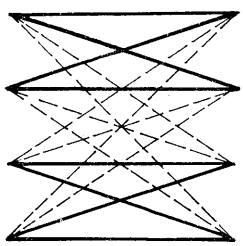


**Fig. 6.** All transitions are from left to right. The solid line transitions have equal probabilities $\frac{1}{2}$. The dashed line transitions have equal probabilities close to 0.

on, are attainable by a suitable choice of $c_1$. The matrix of modulation transition probabilities for $\mathscr{S}_2$ is as follows where the probabilities corresponding to solid lines are (cf. Example 1 and the proof of Proposition 7)

$$\tfrac{1}{2} - \tfrac{1}{2}\Phi(c_2\sqrt{T}),$$

and the probabilities corresponding to dashed lines are

$$\tfrac{1}{2}\Phi(c_2\sqrt{T}).$$

If we take

$$c_2 = \frac{\Phi^{-1}(2\varepsilon)}{\sqrt{T}}, \quad \varepsilon > 0,$$

then the matrix of Figure 6 differs elementwise by $\varepsilon$ from the right-hand matrix of Figure 4. Therefore all paradoxes considered below for $\boldsymbol{P}^*$ and $\boldsymbol{P}^x$ with $M = 4$ apply at least to the alphabets $\mathscr{S}_1$ and $\mathscr{S}_2$ explicitly presented here.

### A. Error versus capacity (information)

It follows from Propositions 8 and 9 that

$$\Delta e(x) \triangleq \frac{e(\boldsymbol{P}^*) - e(\boldsymbol{P}^x)}{e(\boldsymbol{P}^*)} = 1 - 2x$$

and

$$\Delta C(x, M) \triangleq \frac{C(\boldsymbol{P}^*) - C(\boldsymbol{P}^x)}{c(\boldsymbol{P}^*)} = \frac{h(x) + x\log(M-1) - 1}{\log M - 1}.$$

It follows also that $\Delta C(x, M)$ coincides with the relative decrease of information for the uniform probability distribution $\boldsymbol{p}_U$ on signal alphabet, i.e.

$$\Delta C(x, M) = \frac{I(\boldsymbol{p}_U, \boldsymbol{P}^*) - I(\boldsymbol{p}_U, \boldsymbol{P}^x)}{I(\boldsymbol{p}_U, \boldsymbol{P}^*)}.$$

Let us define $0 < x_M < \frac{1}{2}$ by the condition

$$\Delta e(x_M) = \Delta C(x_M, M)$$

and let us put

$$\Delta_M = \Delta e(x_M) = \Delta C(x_M, M).$$

We have found that for every $M$ there is unique $x_M$ and that the values of $x_M$ and $\Delta_M$ are as in Table 1.

**Table 1.**

| $M$ | 3 | 4 | 5 | 6 | 100 | $\infty$ |
|---|---|---|---|---|---|---|
| $x_M$ | 0·3157 | 0·3090 | 0·3081 | 0·3083 | 0·3203 | 0·3333 |
| $100\Delta_M$ | 36·837 | 38·188 | 38·373 | 38·320 | 35·937 | 33·333 |

The conclusions which can be made from these results are the following.

**Proposition 10.** (i) If $M \geqq 3$ then the error decrease can be nearly 100% under the condition that the capacity (information) decrease is positive. This can be achieved by taking $x$ nearly 0.

(ii) If $M \geqq 3$ then the capacity (information) decrease can be nearly $50 \log (M-1)/(\log M - 1)\,\%$ under the condition that the error decrease is positive. This can be achieved by taking $x$ nearly $\frac{1}{2}$. For large $M$ this capacity (information) decrease is nearly 50%.

(iii) If $M = 4$ then the capacity (information) and error can be simultaneously decreased by nearly 40%. This can be achieved by taking $x = 0{\cdot}309$.

### B. Error versus cutoff rate

Let $\Delta e(x)$ be as above and let

$$\Delta R(x, M) = \frac{R(\boldsymbol{P}^*) - R(\boldsymbol{P}^x)}{R(\boldsymbol{P}^*)}.$$

It follows from Proposition 8 and 9 that it holds

$$\Delta R(x, M) = \frac{\log [\sqrt{(1-x)} + \sqrt{(x(M-1))}]^2 - 1}{\log M - 1}.$$

Let us define $0 < x_M < \frac{1}{2}$ by the criterion

$$\Delta e(x_M) = \Delta R(x_M, M)$$

and let us put

$$\Delta_M = \Delta e(x_M) = \Delta R(x_M, M).$$

For every $M$ there is unique $x_M$ which is shown, together with $\Delta_M$, in Table 2.

**Table 2.**

| $M$ | 3 | 4 | $10^2$ | $10^6$ | $10^{20}$ | $10^{90}$ | $\infty$ |
|---|---|---|---|---|---|---|---|
| $x_M$ | 0·244 | 0·228 | 0·170 | 0·91 | 0·035 | 0·010 | 0·000 |
| $100\Delta_M$ | 51·03 | 54·21 | 65·35 | 81·80 | 92·98 | 97·90 | 100·0 |

These results can be summarized in the following form.

**Proposition 11.** (i) The cutoff rate and error can be simultaneously decreased by nearly 100%. This can be achieved by taking $M$ large and $x$ close to 0.

(ii) For every $M \geqq 3$ the cutoff rate and error can be simultaneously decreased by more than 50%. This can be achieved by taking $x = x_M$ shown in Table 2.

### C. Cutoff rate versus capacity (information)

Let $\Delta R(x, M)$ and $\Delta C(x, M)$ be as above, let $x_M$ be defined by the condition

$$\Delta R(x_M, M) = -\Delta C(x_M, M),$$

and let

$$D_M = 100\,\Delta R(x_M, M) = -100\,\Delta C(x_M, M).$$

We have obtained the values presented in Table 3.

**Table 3.**

| $M$ | 3 | 4 | 5 | 6 | 12 | $10^2$ | $10^3$ |
|---|---|---|---|---|---|---|---|
| $x_M$ | 0·172 | 0·124 | 0·101 | 0·080 | 0·040 | 0·008 | 0·0009 |
| $D_M$ | 28·09 | 25·96 | 24·67 | 23·74 | 20·34 | 15·15 | 10·61 |

These results can be presented in words as follows.

**Proposition 12.** It is possible by almost 30% to decrease the cutoff rate and at the same time to increase the capacity and vice versa. This can be achieved by channels $\boldsymbol{P}^*$ and $\boldsymbol{P}^{0.172}$ with $M = 3$. If $M = 4$ then the achievable percentage reduces to about 26%. The percentage $D_M$ achievable for a general $M \geqq 3$ is decreasing with $M$ increasing (cf. Table 3).

It follows from what has been presented in this section that the four procedures
- minimization of $e(\boldsymbol{P})$.
- maximalization of $I(\boldsymbol{p}_U, \boldsymbol{P})$,
- maximization of $C(\boldsymbol{P})$,
- maximization of $R(\boldsymbol{P})$,

yield generally different optimum signal alphabets and that each of the four optimality indices may differ at these alphabets very significantly, sometimes even by almost 100%. An important practical conclusion which follows from here is that the signal alphabet cannot be optimized independently of the secondary digital information processing.

For example, one signal alphabet may be almost 100% worse in cutoff rate. The first alphabet is preferred when error correction is planned by means of a convolutional coding and sequential decoding. The capacity criterion may dominate the scene when long block codes are assumed to be used for error correction.

This area deserves a more systematic attention. For example, the differences between the information optimality criterion $I(\boldsymbol{p}_U, \boldsymbol{P})$ and the capacity criterion $C(\boldsymbol{P})$ is not clear from our study.

An open problem is whether the levels of percentages for controversial relations between various optimality criteria can be exceeded by other examples. Of course, the 100% level of Proposition 11 can hardly be exceeded. Our opinion about the rest

is that the levels of Proposition 10 cannot be exceeded. The remaining ones perhaps can, but not very much. The reason for this belief is that the permutation and symmetric channels have conditional entropies at the theoretically attainable upper and lower bounds for the corresponding conditional error probabilities (cf. [8]). Of course the cutoff rate is directly related neither to the error probability nor to the entropy. Hence we expect slight improvements of levels related to this criterion.

(Received April 9, 1988.)

REFERENCES

[1] E. R. Berlekamp: The technology of error correcting codes. Proc. IEEE *68* (1980), 564—593.
[2] E. Biglieri and M. Elia: Signal sets generated by groups. In: Information Theory Approach to Communications (G. Longo, ed.), Springer-Verlag, New York—Berlin—Heidelberg 1978, pp. 263—306.
[3] R. G. Gallager: Information Theory and Reliable Communication. Wiley, New York 1968.
[4] M. Heyer: Theory of Statistical Experiments. Springer-Verlag, Berlin—Heidelberg—New York 1982.
[5] T. Kailath: RKHS approach to detection and estimation problems. Part I: Deterministic signals in Gaussian noise. IEEE Trans. Inform. Theory *IT-17* (1971), 530—549.
[6] J. L. Massey: Coding and modulation in digital communications. In: Proc. Internat. Zürich Seminar on Digital Communications, Zürich 1974.
[7] D. Slepian: Group codes for the Gaussian channel. Bell System Tech. J. *47* (1968), 575—602.
[8] I. Vajda and K. Vašek: Majorization, concave entropies and comparison of experiments. Problem Control Inform. Theory *14* (1985), 105—115.

*Ing. Igor Vajda, CSc., Ústav teorie informace a automatizace ČSAV (Institute of Information Theory and Automation — Czechoslovak Academy of Sciences), Pod vodárenskou věží 4, 182 08 Praha 8. Czechoslovakia.*