TRANSACTIONS

of the

EIGHTH PRAGUE CONFERENCE

on

INFORMATION THEORY, STATISTICAL DECISION FUNCTIONS, RANDOM PROCESSES

held at

Prague, from August 28 to September 1, 1978

VOLUME C

ACADEMIA

PUBLISHING HOUSE
OF THE
CZECHOSLOVAK ACADEMY OF SCIENCES

PRAGUE 1979

ON AN APPLICATION OF ERGODIC THEORY TO SOME PROBLEMS IN CODING

F. BLANCHARD, D. PERRIN, M.P. SCHÜTZENBERGER

1. INTRODUCTION

Consider a source with alphabet B which is encoded over a channel with alphabet A by means of a mapping

$$\alpha : B \to X$$

of B into a set X of finite strings over the alphabet A.

Moroever a probability μ is defined on the space $B^{\mathbb{Z}}$ of (doubly) infinite strings over B.

This probability induces in a natural way (cf. §3) a probability ν on $A^{\mathbb{Z}}$ and two questions arise :

1. does ν allow to compute μ (source identification problem) ?
2. for which μ is it possible to achieve a stochastic decoding (choosing among the various decodings of a given infinite string in $A^{\mathbb{Z}}$) ?

The question 2 is relevant even if the mapping α is one to one on the set B^* of finite strings over B. In fact, even in this case an infinite string of $A^{\mathbb{Z}}$ may admit various decodings in $B^{\mathbb{Z}}$ and this phenomenon in related to a property of codes called synchronization.

We will show how one may use methods of ergodic theory to answer questions 1 and 2 by assuming convenient hypotheses on the measures μ,ν : this is the transfer theorem of §5.

The terminology and properties of ergodic theory used here may be found in [1]. Proofs will appear elsewhere.

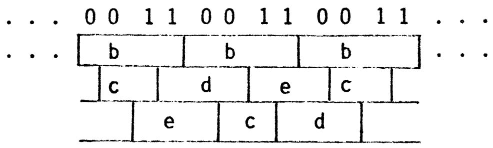
2. EXAMPLE

Let $B = \{a,b,c,d,e\}$, $A = \{0,1\}$ and α be the mapping :

$$\alpha(a) = 0\,0\,0,\quad \alpha(b) = 0\,0\,1\,1,\quad \alpha(c) = 0\,1,\quad \alpha(d) = 1\,0\,0,\quad \alpha(e) = 1\,1\,0.$$

It may be verified that no element of $X = \alpha(B)$ is a left or right factor of another and that α is consequently one to one from B^* into A^*.

Let $G = \{a,b\}^{\mathbb{Z}}$ and H the subset of $B^{\mathbb{Z}}$ of all infinite words that may be written as an infinite product of finite strings taken out of the set $a^*c\,d\,a^*e$. After using the substitution α one obtains the same subset $Z \subset A^{\mathbb{Z}}$ for G and H ; any infinite word in Z can be read in one way as an image of an element of G and in two different ways as the image of an element of H. For instance :



Let ν be a finite ergodic measure on Z distinct of the Dirac measure on the point $0^{\mathbb{Z}}$. Any ergodic measure μ on $B^{\mathbb{Z}}$ such that $\mu^\alpha=\nu$ will have a support included either in G or in H. In fact there is exactly one such measure with $\mu(G) = 1$ and there may be either one or two such measures with $\mu(H) = 1$.

For instance, if μ_1 is such that for almost every element of H, the number of symbols a following an e is odd whereas it is even after a d. Then the equation $\mu^\alpha = \mu_1^\alpha$ has a solution μ_2 which has the reverse property since

$$\alpha(de) = 0\,\alpha(h)0$$

and the parity is inverted between the two intepretations in H.

In this case it is not possible to compute μ knowing ν (i.e. the source may not be idendified) but it is possible to distinguish the two interpretations in H of a given sequence in Z.

3. DEFINITIONS

Let A^* denote the set of finite strings over A ; A^* is the free monoid over the set A.

An encoding

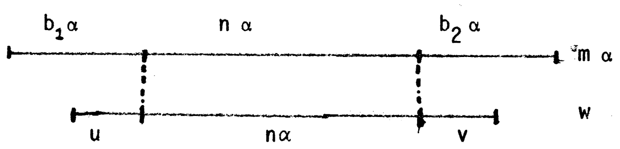
$$\alpha : B \to X \subset A^*$$

is a mapping from B into A^* which can be extended to an injective morphism from B^* into A^*. We suppose A, B and thus X to be finite.

We shall say that a string $m \in B^*$ is a covering of $w \in A^*$ if :

$m = b_1 n b_2$; $b_1, b_2 \in B$

$$f = u(n\alpha)v \ ; \ b_1\alpha \in A^*u \ ; \ b_2\alpha \in vA^*$$



Let $C(w)$ be the set of coverings of w.

Now for any $\mu : B^* \to \mathbb{R}$,

we define $\mu^\alpha : A^* \to \mathbb{R}$

by :

$$\mu^\alpha(w) = \frac{1}{E_\mu(\alpha)} \sum_{m \in C(w)} \mu(m),$$

where $E_\mu(\alpha) = \sum_{b \in B} |b\alpha| \, \mu(b)$ is the average length of $X = B\alpha$.

The following fact is easy to check :

Proposition 1.- If μ defines an invariant or ergodic measure on the space $B^{\mathbb{Z}}$, so does μ^α.

It is convenient to define a subset Ω of $B^{\mathbb{Z}} \times \mathbb{N}$ as follows :

$$\Omega = \{(b,i) \in B^{\mathbb{Z}} \times \mathbb{N} \mid 0 \leq i < f(b)\}$$

where $b = (b_j)_{j \in \mathbb{Z}}$ and $f(b) = |\alpha(b_0)|$ denotes the length of the string $\alpha(b_0) \in A^*$.

The mapping $\alpha : B \to X \subset A^*$ may be extended in a unique way to $\phi : \Omega \to A^{\mathbb{Z}}$

by stipulating that (cf. fig. 1) :

$$\phi(b,i) = \ldots a_{-1}\, a_0\, a_1 \ldots$$

and

$$\begin{cases} \ldots a_{-i-2}\, a_{i-1} = \ldots \alpha(b_{-2})\, \alpha(b_{-1}), \\ a_{-i}\, a_{-i+1} \ldots = \alpha(b_0)\, \alpha(b_1) \ldots \end{cases}$$

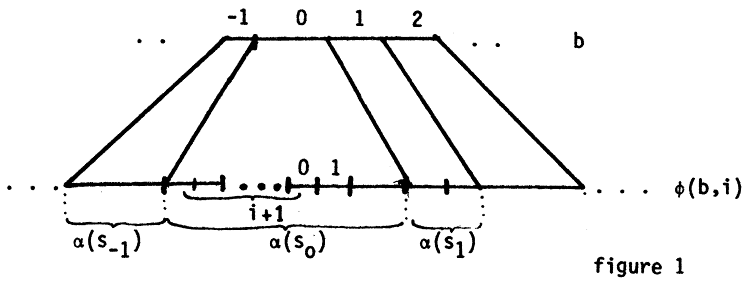


figure 1

An automorphism (i.e. an invertible bimeasurable function) is defined on the set Ω by extension of the natural shift S on $B^{\mathbb{Z}}$:

$$\begin{aligned} \bar{S}(b,i) &= (b,i+1) \quad \text{if } i < f(b) - 1 \\ &= (Sb,0) \quad \text{if } i = f(b) - 1. \end{aligned}$$

In this way, we have a commutative diagram using the shift T on $A^{\mathbb{Z}}$:

$$\begin{array}{ccc} \Omega & \xrightarrow{\phi} & A^{\mathbb{Z}} \\ \downarrow \bar{S} & & \downarrow T \\ \Omega & \xrightarrow{\phi} & A^{\mathbb{Z}} \end{array}$$

This construction is just that of the standard <u>tower</u> of height f over the space $B^{\mathbb{Z}}$; and the measure μ^α defined above is nothing else than the measure induced by ϕ on $A^{\mathbb{Z}}$ from the restriction to Ω of the product measure on $B^{\mathbb{Z}} \times \mathbb{N}$.

One may also note that the image of Ω in $A^{\mathbb{Z}}$ by ϕ is a sofic system, as defined by B. Weiss [4] ; in fact, it is classical that if X is a finite set, there exists a finite monoid M and a morphism

$$\sigma : A^* \to M$$

such that $\sigma^{-1}\sigma X^* = X^*$ (cf. [3], for instance).

4. INTERPRETATIONS

Given an $a \in A^{\mathbb{Z}}$, we say that $I \subset \mathbb{Z}$ is an <u>interpretation</u> of a if for any consecutive elements n,m in I, one has :

$$a_n\, a_{n+1} \cdots a_{m-1} \in X.$$

Thus, for example, for any $(b,i) \in \Omega$, the element $\phi(b,i)$ admits an interpretation containing the point $-i$.

<u>Proposition 2</u>.- Let ν be a shift invariant measure on $A^{\mathbb{Z}}$ whose support is included in $\phi(\Omega)$; for almost any point in $A^{\mathbb{Z}}$, two distinct interpretations have an empty intersection.

If ν is ergodic, the number of interpretation is almost surely constant.

It is worthwhile to mention that both statements of this proposition have an algebraic counterpart. The second one is related to the Suschkevitch theorem in finite monoids (cf. [2]) and the first one may be restated as follows :

Say that a $A^{\mathbb{Z}}$ is <u>formally recurrent</u> if any finite factor

$$w = a_i\, a_{i+1} \cdots a_{i+j}$$

occurring in a may be found infinitely many times for $i \geq 0$ and for $i \leq 0$.

<u>Proposition 3</u>.- Two distinct interpretations of a formally recurrent sequence are disjoint.

Let us now suppose that ν is an ergodic measure on $A^{\mathbb{Z}}$; we call <u>degree of the channel</u> the integer $d = d(\alpha,\nu)$ which is the number of interpretations of almost every point in $A^{\mathbb{Z}}$; E is the set of these points.

The set $E \times \bar{d} = E \times \{1,2,\ldots,d\}$ is equipped with a bimeasurable bijection $\tilde{T}$ making the following diagram commute :

$$\begin{array}{ccc} \Omega & \xrightarrow{\ \eta\ } & E \times \bar{d} \\ \bar{S} \downarrow & & \downarrow \tilde{T} \\ \Omega & \xrightarrow{\ \eta\ } & E \times \bar{d} \end{array}$$

where $\eta(b,i) = (\phi(b,i),j)$, with j determinated by an arbitrary ordering of the set of interpretations of $a = \phi(b,i)$.

In this way, $\tilde{T}(a,j) = (Ta, p_a(j))$

where p_a is a permutation.

If we are given an ergodic measure μ on $B^{\mathbb{Z}}$ such that $\mu^{\alpha} = \nu$, we may define the <u>degree of the source</u> using the following statement :

<u>Proposition 3</u>.- **There exists an event $P \subset \Omega$ with measure 1 such that for any a in E, the cardinality of the set**

$$\{j \in \bar{d} \mid (a,j) \in \eta P\}$$

is almost surely constant.

We denote by $d' = d'(\alpha,\mu)$ this integer, which is by definition the degree of the source ; it is obviously the number of interpretations of an element of $A^{\mathbb{Z}}$, coherent with the measure μ. These interpretations may be asymptotically discriminated from the others, considering only finite strings of A^*.

5. TRANSFER THEOREM

Denote by $\tilde{\nu}$ the measure on $E \times \bar{d}$ which is the product of the ergodic measure ν by the measure giving weight $1/d$ to each point of $\bar{d}$.

<u>Proposition 4</u>.- **The measure $\tilde{\nu}$ is invariant by $\tilde{T}$**

We can now state the main result of this paper which may be considered as a transfer theorem from the ergodic measures on $A^{\mathbb{Z}}$ to that on $B^{\mathbb{Z}}$ by means of the encoding :

<u>Theorem</u>. - **The ergodic measures μ on $B^{\mathbb{Z}}$ solution of**

$$\mu^{\alpha} = \nu$$

are elements of the set M of ergodic decomposition of $\tilde{\nu}$. Moroever :

$$\sum_{\mu \in M} d'(\alpha,\mu) = d.$$

In other words if μ is an ergodic measure inducing by α the measure $\mu = \nu^{\alpha}$, an element of $A^{\mathbb{Z}}$ admits $d' = d'(\alpha,\mu)$ indistinguishable interpretations.

Thus the source identification problem is easiest when $d'=d$ whereas stochastic decoding is of maximal complexity. Conversely, when $d'=1$, the number of possible sources is d but for a given source stochastic decoding may be achieved unambiguously.

REFERENCES

[1] BILLINGSLEY, P. : Ergodic Theory and Information
Wiley, 1965.

[2] CLIFFORD, A.H. et C.B. PRESTON : The Algebraic Theory of Semigroups
Vol. 1 , Amer. Math. Soc. (1961).

[3] EILENBERG, S. : Automata, Languages and Machines, Vol. A
Academic Press, (1974).

[4] WEISS, B. : Subshifts of finite type and sofic systems,
Monatshefte für Math., 77 (1973) 462-474.

F. BLANCHARD
UNIVERSITE PARIS VI
LABORATOIRE DE PROBABILITES
Tour 56
4 Place Jussieu
75230 PARIS CEDEX 05

D. PERRIN
UNIVERSITE DE ROUEN
et LABORATOIRE C N R S
Informatique théorique et
Programmation

M.P. SCHÜTZENBERGER
UNIVERSITE PARIS VII
et L I T P