1er COLLOQUE AFCET-SMF DE MATHÉMATIQUES APPLIQUÉES

FIRST MEETING AFCET-SMF ON APPLIED MATHEMATICS

4-8 Septembre 1978

Ecole Polytechnique
PALAISEAU (FRANCE)

Tome I

CONFERENCES - INVITED PAPERS
COMMUNICATIONS THEMES I, II

AFCET : Association Française pour la Cybernétique Économique et Technique
156, boulevard Péreire
B.P. 571
75826 Paris Cédex 17

SMF : Société Mathématique de France
11, rue Pierre et Marie Curie
75231 Paris Cédex 05

UNE APPLICATION DE LA THEORIE ERGODIQUE AU PROBLEME DU CODAGE

F. BLANCHARD
Université Paris VI

D. PERRIN
Université de Rouen

M.P. SCHÜTZENBERGER
Université Paris VII

1. INTRODUCTION

On étudie ici les problèmes soulevés par le codage sur des mots (doublement) infinis et on emploie pour cela des notions et des résultats empruntés à la théorie ergodique.

On se donne un codage (i.e. un morphisme injectif)

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

que l'on étend de façon naturelle aux suites infinies de $B^{\mathbb{Z}}$. Il n'est alors en général plus injectif puisque si, par exemple, $B = \{u,v\}$ $A = \{a,b\}$ et :

$$\alpha : \ u \longmapsto ab, \quad v \longmapsto ba,$$

le mot $(ab)^{\mathbb{Z}}$ admet deux décodages : $u^{\mathbb{Z}}$ ou $v^{\mathbb{Z}}$.

Ce phénomène correspond à un problème bien connu en théorie des automates : c'est l'étude des sous-groupes du monoïde syntaxique d'un langage et, en particulier, le problème de la synchronisation des codes .

Nous l'abordons ici sous l'aspect des probabilités : on se donne une mesure P sur $B^{\mathbb{Z}}$ qui induit par α une mesure

$$Q = P^{\alpha}$$

sur $A^{\mathbb{Z}}$ ayant les mêmes propriétés d'invariance ou d'ergodicité (cf. § 2). Il peut sembler intuitif que, même si un ensemble de mots de $A^{\mathbb{Z}}$ admet plusieurs décodages en sous ensembles de $B^{\mathbb{Z}}$, l'un de ceux-ci soit plus probable que les autres. Le résultat principal de cet article établit que ceci est, en un sens, exact dans le cas où l'équation en P :

$$P^{\alpha} = Q$$

admet le nombre maximum de solutions . On peut faire apparaître ce résultat comme une sorte de relation d'incertitude reliant l'inambiguité (stochastique) du décodage à la possibilité d'identifier la source (i.e. de déterminer P à partir de Q).

Nous remercions F. Ledrappier de nous avoir aidé à simplifier la démonstration de la prop. 10.

2. NOTATIONS

On note A^* le monoïde libre sur A et $A^+ = A^* \setminus 1$ le semi-groupe libre sur A. On considère un morphisme

$$\alpha : B^* \to A^*.$$

On dira que c'est un codage s'il est injectif de B^* dans A^*. La partie $X = B\alpha$ de A^* est alors, par définition, un code. On suppose ici que B, A et donc X sont des ensembles finis.

On notera $\mathcal{R} = X(A^+)^{-1} = \{ p \in A^* \mid pA^+ \cap X \neq \emptyset \}$ l'ensemble des préfixes de X et

$$\mathcal{S} = (A^+)^{-1} X = \{ q \in A^* \mid A^+ q \cap X \neq \emptyset \}$$ l'ensemble de ses suffixes.

Etant donné un morphisme $\alpha : B^* \to A^*$, une interprétation d'un mot $w \in A^*$ est un triplet $y = (q, b, p)$ de $\mathcal{S} \times B^* \times \mathcal{R}$ tel que $w = q.b\alpha.p$.

Maintenant si on dispose d'une application,

$$P : B^* \to \mathbb{R}$$

on définit une nouvelle application :

$$P^\alpha : A^* \to \mathbb{R}$$

que l'on dira induite par α, de la façon suivante :

$$P^\alpha(w) = \sum P(b_1 b b_2)$$

où la somme porte sur les triplets (b_1, b, b_2) tels que w admet une interprétation (q, b, p) et $b_1 = 1$ (resp. $b_2 = 1$) si $q = 1$ (resp. $p = 1$), $b_1 \in B$, $b_1\alpha \in A^*q$ sinon (resp. $b_2 \in B$, $b_2\alpha \in pA^*$).

Supposons maintenant que l'on utilise P pour définir sur l'espace $B^{\mathbb{Z}}$ une mesure. Elle induit une mesure P^α sur $A^{\mathbb{Z}}$ et l'on a :

<u>**Proposition 1**</u> : *Si P définit une mesure invariante ou ergodique, il en est de même de P^{α}, pour tout morphisme α de B^* dans A^*.*

Pour établir ce résultat, il suffit de montrer que la construction de P^{α} coïncide avec la construction habituelle d'une tour au dessus de $B^{\mathbb{Z}}$.

Il est commode de définir pour cela une partie Ω de $B^{\mathbb{Z}} \times \mathbb{N}$:

$$\Omega = \{ (b, i) \in B^{\mathbb{Z}} \times \mathbb{N} \mid 0 \leq i \leq f(b) - 1 \}$$

ou $b = (b_j)_{j \in \mathbb{Z}}$ et $f(b) = | b_0\alpha |$ est la longueur du mot $b_0 \alpha \in A^*$.

On étend l'application α en une application

$$\varphi : \Omega \longrightarrow A^{\mathbb{Z}}$$

définie ainsi : pour $b \in B^{\mathbb{Z}}$ et $i \in \mathbb{N}$ on pose

$$\begin{cases} b_0\alpha \,.\, b_1\alpha \,.\, b_2\alpha \ldots = a_{-i}\, a_{-i+1}\, a_{-i+2} \ldots\ldots \\ \ldots b_{-2}\alpha\, b_{-1}\alpha = \ldots a_{-i-2}\, a_{-i-1} \,. \end{cases}$$

Un automorphisme $\bar{\sigma}$ est défini sur Ω par extension du shift sur $B^{\mathbb{Z}}$:

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

Cela donne un diagramme commutatif utilisant le shift τ de $A^{\mathbb{Z}}$:

$$\begin{array}{ccc} \Omega & \xrightarrow{\varphi} & A^{\mathbb{Z}} \\ {\scriptstyle \bar{\sigma}}\downarrow & & \downarrow{\scriptstyle \tau} \\ \Omega & \xrightarrow{\varphi} & A^{\mathbb{Z}} \end{array}$$

Cette construction n'est autre que celle de la tour de hauteur f au dessus de l'espace $B^{\mathbb{Z}}$; la mesure P^{α} définie précédemment coïncide avec la mesure induite par φ sur $A^{\mathbb{Z}}$ à partir de la restriction à Ω de la mesure produit sur $B^{\mathbb{Z}} \times \mathbb{N}$. Il est classique (et facile à vérifier) que cette mesure possède relativement au shift $\bar{\sigma}$ les propriétés indiquées dans la proposition 1. L'hypothèse que α est injective sur B^*, c'est-à-dire que α est un codage, n'est pas nécessaire pour obtenir ce résultat.

Si P est une mesure de probabilité, alors

$$\frac{1}{E_\rho(\alpha)} \; P^\alpha$$

est une mesure de probabilité sur $A^{\mathbb{Z}}$, où $E_\rho(\alpha) = \sum_{b \in B} |b\alpha| \, \rho(b)$ est la longueur moyenne de X.

3. INTERPRETATIONS

Pour une suite infinie $a \in A^{\mathbb{Z}}$ nous définissons une interprétation de a (relative à un morphisme α) comme un ensemble $I \subset \mathbb{Z}$ tel que pour deux éléments consécutifs $n,m \in I$, on a :

$$a_n \, a_{n+1} \dots a_{m-1} \in X = B\alpha \; .$$

On remarquera que cette définition est cohérente avec celle des interpretations d'un mot $w \in A^*$.

L'ensemble des suites qui ont au moins une interprétation est l'image par φ de Ω ; la proposition suivante montre que l'appartenance d'une suite à cet ensemble ne dépend que de ses facteurs finis :

Proposition 2 : *Une suite* $a \in A^{\mathbb{Z}}$ *est dans* $\Omega\varphi$ *ssi tous ses facteurs* $w \in A^*$ *sont dans l'ensemble :*

$$W(X^*) = (A^*)^{-1} X^* (A^*)^{-1} = \{ w \in A^* \mid A^* w A^* \cap X^* \neq \emptyset \}.$$

Démonstration : La condition est certainement nécessaire ; elle est suffisante puisqu'à toute suite $a \in A^{\mathbb{Z}}$ ayant tous ses facteurs dans l'ensemble $W(X^*)$ on peut faire correspondre une suite $(b^{(n)})_{n \in \mathbb{N}}$ d'éléments de $B^{\mathbb{Z}}$ telle que : $a_{-n} \, a_{-n+1} \dots a_{n-1} \, a_n$ soit facteur de $b^{(n)}\alpha$. Comme B est fini, on peut extraire de cette suite une sous-suite convergente ; sa limite est un élément de $a\varphi^{-1}$ $\square$

Ce résultat montre que l'ensemble $\Omega\varphi$ (qui contient le support de P^α) est un "sofic system" au sens de B Weiss. En effet, il est bien connu que si X est fini, il existe un morphisme

$$\gamma : A^* \longrightarrow M$$

sur un monoïde fini M tel que $\gamma^{-1}\gamma X = X$. On peut, par exemple, prendre pour M le monoïde des relations sur l'ensemble (fini) R des préfixes de X et définir l'image par γ d'une lettre $a \in A$ comme la relation constituée des couples (p, pa) pour tout $p \in R$ tel que $pa \in R$ et des $(p, 1)$ pour tout $p \in R$ tel que $pa \in X$. Une telle construction est possible plus généralement quand X est reconnaissable (cf. [5] par exemple).

Nous donnons maintenant deux énoncés portant sur l'ensemble des interprétations d'une suite $a \in A^{\mathbb{Z}}$. Nous supposons pour cela dorénavant que α est un codage.

Le nombre d'interprétations (q, b, p) d'un mot $w \in A^*$ est borné puisque le couple $(q, p) \in S \times R$ détermine $b \in B^*$:

$$q.b\alpha.p = q.b'\alpha.p \Rightarrow b\alpha = b'\alpha \Rightarrow b = b'.$$

La proposition suivante montre que le nombre d'interprétations d'une suite infinie $a \in A^{\mathbb{Z}}$ est fini :

Proposition 3 : *Le nombre d'interprétations de* $a \in A^{\mathbb{Z}}$ *est la limite inférieure du nombre d'interprétations de ses facteurs de la forme :*

$$w_n = a_{-n}\, a_{-n+1} \dots a_{n-1}\, a_n .$$

Démonstration : Si d(a) (resp. d(w)) est le nombre d'interprétations de $a \in A^{\mathbb{Z}}$ (resp. de $w \in A^*$), on a certainement

$$d(a) \leqslant d(w_n)$$

pour tout entier $n \geqslant n_o$, où n_o est le plus grand élément des $I \cap J$ pour tout couple I,J d'interprétations distinctes de a. Et si k est un point d'accumulation de la suite $d(w_n)_{n \in \mathbb{N}}$, on montre, comme dans la preuve de la proposition 2, que la suite a a k interprétations distinctes □

Le nombre d'interprétations disjointes d'une suite apériodique est borné par le cardinal de B (i.e. le nombre d'éléments de X) ; on pourra à ce sujet consulter les importants résultats de J.P. Duval [4].

La propriété suivante montre en particulier que (pour une mesure invariante) deux interprétations distinctes d'une même suite sont presque sûrement disjointes. On verra au paragraphe suivant une preuve directe de ce fait.

On dira qu'une suite $a \in A^{\mathbb{Z}}$ est *formellement récurrente* si tout facteur

$$w = a_i\, a_{i+1} \dots a_{i+j} , \quad i \in \mathbb{Z} , \; j \in \mathbb{N} ,$$

peut être trouvé une infinité de fois pour $i \geqslant 0$ et pour $i \leqslant 0$.

Proposition 4 : *Deux interprétations distinctes d'une suite formellement récurrente sont disjointes.*

Démontration : Nous établissons tout d'abord l'énoncé suivant :

<u>Lemme 1</u> : *Soit* γ *un morphisme de* A^* *sur un monoïde fini* M *; si* a *est formellement récurrente, il existe une partie* I *de* $\mathbb{Z}$ *et un idempotent* u *de* M *tels que pour deux éléments consécutifs* i,j *de* I *, on ait :*

$$(a_i\, a_{i+1} \dots a_j)\gamma = u .$$

<u>Démonstration</u> : Soit K le plus petit idéal de M qui contient l'image par φ d'au moins un facteur de a , et n un entier tel que :

$$g = a_{-n} \dots a_{-2}\, a_{-1} , \quad g\gamma \in K .$$

Maintenant il existe au moins un intervalle positif qui est le support du même mot et donc un entier m tel que :

$$g' = a_o\, a_1 \dots a_m , \quad g'\gamma \in K .$$

Soit alors $(H_t)_{t \in \mathbb{Z}}$ une suite d'intervalles disjoints qui sont le support du mot h = gg' ; si on note U_t l'intervalle de $\mathbb{Z}$ qui sépare H_t de H_{t+1} et u_t le mot dont il est le support, on a alors :

$$a_o\, a_1\, a_2 \dots = g'\, u_1\, gg'\, u_2\, gg'\, u_3\, gg' \dots$$

de sorte que $\mathbb{Z}$ est partitionné en une suite d'intervalles disjoints de la forme $(H''_t \cup U_t \cup H'_{t+1})$ où $H_t = H'_t \cup H''_t$, et H'_t (resp. H''_t) est le support de g (resp. g'). D'autre part, d'après le lemme de Green (cf. [3]), les mots $v_t = g'u_t g$ ont une image par γ équivalente par la relation $\mathcal{H}$ à celle de g'g :

$$v_t\gamma\, \mathcal{H} (g'g)\gamma .$$

Notons $v = (v_t)_{t \in \mathbb{Z}}$ et considérons la fonction ν définie sur lès facteurs de v par :

$$\nu(v_i\, v_{i+1} \dots v_{i+j}) = \text{Card}\left\{ (v_{i+k} \dots v_{i+j})\gamma \,|\, 0 \leqslant k \leqslant j \right\}.$$

On choisit un facteur

$$h = v_i\, v_{i+1} \dots v_{i+j}$$

de v tel que $\nu(h)$ soit maximal. Comme a est formellement récurrent, on peut écrire :

$$a = \dots h\, r_{-1}\, h\, r_o\, h\, r_1\, h\, r_2\, h \dots\dots \qquad \text{ou } r_i \text{ est}$$

facteur de v . Maintenant, pour tout entier k , $0 \leqslant k \leqslant j$ et tout $t \in \mathbb{Z}$, il existe un entier k' tel que : $(v_{i+k} \dots v_{i+j}\, r_t\, h)\gamma = (v_{i+k'} \dots v_{i+j})\gamma$.

Cela implique que $v_{i+k} \dots v_{i+j}\, r_t\, v_i \dots v_{i+k'-1}$ ait une image par γ égale à l'idempotent contenu dans la $\mathcal{H}$-classe de g'g et établit le lemme □

Considérons maintenant le morphisme γ de A^* dans le monoïde des relations sur l'ensemble $R = X(A^+)^{-1}$ des préfixes de X défini ci-dessus. On a l'équivalence suivante, pour tout mot $w \in A^*$:

$$(p, p') \in w\gamma \iff pw \in X^* p' .$$

Nous démontrons l'énoncé suivant qui est établi en [2] dans un cadre plus général :

<u>Lemme 2</u> : *Si* $w\gamma$ *est idempotent, et si* $(p, p') \in w\gamma$, *il existe un unique* $u \in P$ *tel que*

$$(p, u),\ (u, p') \in w\gamma ;$$

on a de plus $(u, u) \in w\gamma$.

<u>Démonstration</u> : Puisque $w\gamma = w^2\gamma$, il existe au moins un $u \in R$ tel que :

$$(p, u),\ (u, p') \in w\gamma ;$$

et s'il en existait un autre, soit u', on obtiendrait deux interprétations du mot pw^2 qui sont $(1, (xy)\alpha^{-1}, p')$ et $(1, (x'y')\alpha^{-1}, p')$ avec :

$$pw = xu,\quad uw = yp' ,\quad pw = x'u' ,\quad u'w = y'p'.$$

Du fait que ces interprétations sont égales, on obtient $u = u'$.

Enfin, comme $w^2\gamma = w^3\gamma$, il existe un $u' \in P$ tel que :

$$(p, u),\ (u, u'),\ (u', p') \in w\gamma.$$

Mais on obtient alors aussi $(p, u') \in w\gamma$, et l'unicité de u implique $u = u'$ □

Nous terminons maintenant la preuve de la proposition 4 : soit a une suite formellement récurrente et J, K deux interprétations de a qui possèdent en commun le point $i \in J \cap K$. On peut alors trouver une partie I de $\mathbb{Z}$ contenant le point i satisfaisant les hypothèses du lemme 1 ; d'après le lemme 2, l'ensemble I est contenu tout entier dans $J \cap K$, ce qui montre que $J = K$ et démontre le résultat.

4. CONSTRUCTIONS D'ESPACES MESURABLES

Nous avons vu qu'une mesure de probabilité P ergodique sur $B^{\mathbb{Z}}$ se transporte en une mesure ergodique P^{α} sur $A^{\mathbb{Z}}$. Avant d'attaquer le problème inverse, introduisons un certain nombre d'espaces isomorphes à Ω .

A) Soit Σ l'ensemble des parties de $\mathbb{Z}$ de bornes $-\infty$ et $+\infty$. Il est muni de la tribu $\mathcal{T}$ rendant mesurable le nombre de points de la partie I dans tout intervalle de $\mathbb{Z}$; si I_o est le premier point de I d'abscisse négative, les autres étant numérotés à partir de celui-ci dans l'ordre croissant, $\mathcal{T}$ est aussi la plus petite tribu rendant mesurables les applications

$$I \longrightarrow I_k \quad , \quad k \in \mathbb{Z} \ .$$

Σ est muni de la translation

$I \longrightarrow I-1$, qui est une bijection bimesurable.

<u>Définitions</u> : On dira que $I \in \Sigma$ et $y \in A^{\mathbb{Z}}$ sont <u>compatibles</u> si I est une interprétation de y . Si $t \in I$, t est une <u>scansion</u> de y ou de (y,I) .

L'ensemble Ω' des couples compatibles est une partie mesurable de $(A^{\mathbb{Z}} \times \Sigma \ , \ \mathcal{A} \otimes \mathcal{T})$.

Munissons donc Ω' de la restriction $\mathcal{F}'$ de $\mathcal{A} \otimes \mathcal{T}$. Ω' est muni en outre de l'application bijective bimesurable ν :

$$\nu(y,I) \ = \ (\tau y, I-1) \ .$$

Ainsi défini, $(\Omega', \mathcal{F}', \nu)$ est isomorphe à $(\Omega, \mathcal{F}, \bar{\sigma})$ à une condition près :

<u>Proposition 5</u> : *Si* $\alpha_{|B}$ *est une injection, il existe une bijection bimesurable* $\psi_1 : \Omega \to \Omega'$ *telle que*

$$\nu \circ \psi_1 \ = \ \psi_1 \circ \bar{\sigma} \ .$$

Démonstration : Posons

$$\psi_1(x,i) = (\phi(x,i)\ ,\ \{f_k(x)-i\ ,\ k \in Z\})\ .$$

ψ_1 est mesurable. L'application qui à (y,I) fait corespondre a) le point de $B^{\mathbb{Z}}$ de coordonnées $x_k = \alpha^{-1}(y_{I_k} \dots y_{I_{k+1}} -1)$, où x_k est bien défini grâce à notre hypothèse, et b) l'entier $-I_o$, est inverse de ψ_1 et mesurable. La dernière relation se vérifie à la main ∎

Nous savons qu'il peut y avoir plusieurs relèvements d'un point y de $A^{\mathbb{Z}}$ dans Ω' : appelons Ω'_y l'ensemble de ces relèvements (qui est fini et même borné dès que α est un codage) .

Proposition 6 : *Soit α un codage de B^* dans A^* . 1) L'application d' : $A^Z \to \mathbb{N}$*

$d'(y) = card\ (\Omega'_y)$

est mesurable.

2) L'ensemble des points de $A^{\mathbb{Z}}$ ayant au moins deux interprétations (y,I) et (y,I') telles que $I \cap I' \neq \emptyset$ est mesurable.

Démonstration :

1) résulte immédiatement de la proposition 3 .

2) entrainé par un argument analogue ∎

B) Nous nous intéressons maintenant à l'ensemble $E(d',\alpha) = E_{d'}$ des mots infinis de A^Z ayant exactement d'interprétations deux à deux disjointes. D'après la proposition, les mots formellement récurrents sont dans $E_{d'}$. Nous venons de démontrer que $E_{d'}$ est mesurable dans $(A^Z, \mathfrak{a})$. Posons

$$\Omega_{d'} = \phi^{-1}(E_{d'})\ ,\ \text{et}$$
$$\bar{d}' = \{o,1, \dots d'-1\} \text{ pour } d' \in \mathbb{N}\ .$$

Proposition 7 : *Soit α un codage, d'un entier strictement positif tel que $E_{d'} \neq \emptyset$. Il existe alors une bijection bimesurable*

$$\psi : \Omega_{d'} \longrightarrow \Omega''_{d'} = E_{d'} \times \bar{d}'\ ,$$

et une bijection bimesurable $\tilde{\tau}$ de $E_{d'} \times \bar{d}' = \Omega''_{d'}$,

$$\tilde{\tau} = \psi_o \bar{\sigma}_o \psi^{-1} , \quad \text{telle que}$$

1) l'application coordonnée de ψ dans $E_{d'}$ coïncide avec ϕ .

2) $\tilde{\tau}(y,i) = (\tau y, p(y,i))$ où $p(y,\cdot)$ est une permutation sur $\overline{d'}$.

Démonstration :

1) Il nous suffit d'exhiber une bijection convenable de $\Omega'_{d'} = \psi_1(\Omega_{d'})$ dans $E_{d'} \times \overline{d'} = \Omega''_{d'}$ pour obtenir

$$\psi = \psi_2 \circ \psi_1 .$$

L'application coordonnée de ψ_2 dans $E_{d'}$ est l'identité. Considérons $y \in E_{d'}$, et ses d' interprétations distinctes, qui n'ont pas de scansion commune ; soit comme plus haut

$$I_o = \sup \{t \in I : t<o\} .$$

Rangeons les d' interprétations dans l'ordre décroissant de leurs I_o respectifs, ce qui est possible puisqu'elles n'ont pas de scansions communes : ceci définit une application de Ω'_y dans $\{y\} \times \overline{d'}$, qui est bijective, et appelons ψ_2 l'application correspondante de Ω' dans $\Omega''_{d'}$. La mesurabilité de ψ_2 et ψ_2^{-1} s'obtient de façon simple. La première coordonnée de ψ est ϕ .

2) Par conséquent $\tilde{\tau}(y,i) = (\tau y, j)$. Pour identifier la seconde coordonnée, deux cas sont à distinguer :

a) sur $\{(y,j) : 1 \notin \bigcup_{I : (y,I) \in \Omega'} I\}$, on a

$$\tilde{\tau}(y,j) = (\tau y, j) .$$

L'action de ν ne modifie pas l'ordre des interprétations.

b) sur $\{(y,j) : \exists_k \in \overline{d'} : 1 \in I_k\}$, l'ordre des interprétations est modifié par ν de la façon suivante :

$$p(y,j) = \begin{cases} j+1 & \text{pour } o \leq j < i \\ 0 & \text{pour } j = i \\ j & \text{pour } j > i \end{cases}$$

La mesurabilité des deux ensembles considérés, et celle de la variable partielle i définie ci-dessus, découlent immédiatement de la définition des tribus utilisées ∎

5. DEGRE DU CANAL.

Supposons qu'étant donnée une mesure ergodique Q sur A^Z, nous connaissions déjà une mesure R sur $\Omega''_{d'}$, dont elle soit l'image sur la première coordonnée. Nous allons voir d'abord que l'application ψ^{-1} permet de ramener R sur Ω, après quoi on lui associe une mesure ergodique P unique sur B^Z. Toutes les mesures considérées seront des probabilités.

Proposition 8 : *Soit* α *un codage de* B^* *dans* A^*, Q *une mesure invariante sur* $A^{\mathbb{Z}}$, *ne chargeant que* $\phi(\Omega)$.

1) Alors, pour presque tout point de $A^{\mathbb{Z}}$, *deux interprétations distinctes sont disjointes.*

2) Si de plus Q *est ergodique, le nombre d'interprétations distinctes est presque surement constant.*

Démonstration :

1) Il suffit de remarquer que, grâce à la stationnarité, presque tous les mots sont formellement récurrents, et d'appliquer la proposition 4. On peut aussi le démontrer sans utiliser la propriété de récurrence formelle.

2) Le nombre d'interprétations distinctes est mesurable (proposition 6) et invariant par τ, donc presque surement constant si Q est ergodique ∎

Cette proposition signifie que l'application ϕ est presque partout définie et ne fait intervenir qu'un ensemble $\Omega''_{d'}$. Appelons degré du canal l'entier $d' = d'(\alpha,Q)$ associé par la proposition précédente à la mesure Q .

6. DECODAGE ET IDENTIFICATION DE LA SOURCE.

Le problème qu'il nous reste à résoudre consiste, étant donnée une mesure ergodique Q sur $A^{\mathbb{Z}}$, à la remonter en une mesure ergodique sur $\Omega''_{d'}(\alpha,Q)$.

Appelons η l'application coordonnée de $\Omega''_{d'}$ dans $E_{d'}$, et $\tilde{Q}$ la mesure sur $\Omega''_{d'}$:

$$\tilde{Q} = \frac{1}{d'} Q \otimes \left(\sum_{i \in \overline{d'}} \delta_i \right).$$

Proposition 9 : *La mesure* $\tilde{Q}$ *est invariante par* τ *; la tribu de ses invariants* $\mathcal{J}$ *est atomique et compte au plus* d' *atomes.*

Démonstration : $\tilde{\tau}$ est le produit de la transformation τ, qui conserve Q, par des permutations de $\overline{d'}$. Elle laisse donc $\tilde{Q}$ invariante.

Supposons qu'il existe un ensemble invariant E mesurable dans $\Omega''_{d'}$, tel que

$$0 < \tilde{Q}(E) < \frac{1}{d'}.$$

On peut trouver j dans $\overline{d'}$, tel que

$$\tilde{Q}\{(y,j) \ : \ (y,j) \in E\} \neq 0 .$$

Alors le sous-ensemble $\eta(E)$ de $E_{d'}$, de mesure $Q(\eta(E)) \leq d' \cdot \tilde{Q}(E) < 1$, est invariant par τ, ce qui contredit l'ergodicité de la mesure Q pour τ ∎

Remarque : On voit facilement qu'à chaque y, pour un ensemble invariant E, est associé un entier positif $d'' = \mathbf{card}\{(y,i) \ : \ (y,i) \in E\}$, qui est presque surement constant.

Voici maintenant le résultat principal de cet article. Il est énoncé sous sa forme la plus abstraite, nous expliquerons ensuite ce qu'il signifie.

Proposition 10 : *Soit* α *un codage,* Q *une mesure ergodique finie sur* $A^{\mathbb{Z}}$*, ne chargeant que l'ensemble* $E_{d'}$. *Les mesures ergodiques* R *sur* $(\Omega''_{d'}, \tilde{\tau})$ *de marginale* Q *sont, à un coefficient près, les restrictions de* $\tilde{Q}$ *aux atomes de sa tribu invariante. Les entiers* $d''(\alpha,R)$ *associés à* *chacune d'entre elles d'après la remarque précédente vérifient*

$$(2) \qquad \sum_{\{R:R\nu^{-1}=Q\}} d''(\alpha,R) = d'(\alpha,Q) \ .$$

Cette proposition répond aux deux questions que nous nous sommes posées :

1) Celle de l'identification de la source a au moins 1 et au plus $d'(\alpha,Q)$ solutions, suivant la structure de $\tilde{Q}$.

2) Celle de l'ambiguïté du décodage : presque tout mot y de $A^{\mathbb{Z}}$ a d'' interprétations "probables", et d'' est compris entre 1 et d' .

Si on suppose que la mesure R provient d'une mesure P sur $B^{\mathbb{Z}}$, nous appellerons $d'' = d''(\alpha,P)$ degré de la source P .

3) Enfin, globalement, le décodage est d'autant moins ambigu que le nombre de solutions de l'équation $P^{\alpha} = Q$ est plus proche de d' , donc l'identification de la source plus difficile.

On peut donner de la réponse à la question du décodage une interprétation finitiste. Soit $y \in E_{d'}$, et $\{A_n\}$ la suite décroissante d'événements mesurables

$$A_n = \{z \in E_{d'} \ : \ z_n = y_{-n} \ , \ z_{-n+1} = y_{-n+1} \ \dots \ z_n = y_n\} \ .$$

Soit P une mesure ergodique sur $B^{\mathbb{Z}}$, $R = P_o\psi^{-1}$, $Q = P^{\alpha}$. Le théorème des martingales affirme que la suite

$$d' \ \frac{R(A_n\times\{i\})}{Q(A_n)} = \frac{R(A\times\{i\})}{\tilde{Q}(A_n\times\{i\}} \ , \ n \in \mathbb{N}$$

tend pour presque tout y quand $n \to +\infty$ vers $\frac{dR}{d\tilde{Q}}(y,i)$, c'est-à-dire vers $\frac{d'}{d''}$ ou 0 , suivant que (y,i) fait ou non partie du support de R . C'est-à-dire que connaissant un segment fini mais suffisamment long du mot y, on pourra distinguer les interprétations "probables" au sens de P de celles qui ne le sont pas.

Démonstration de la proposition 10 :

1) a) Soit R telle que $R\circ\eta^{-1} = Q$.

Ceci implique que R est absolument continue par rapport à $\tilde{Q}$: donc la dérivée $\frac{dR}{d\tilde{Q}}$ existe, et c'est une fonction presque surement invariante par $\tilde{\tau}$. Elle est donc constante sur chacun des atomes de la tribu $\mathfrak{J}$ des invariants de $\tilde{\tau}$ pour $\tilde{Q}$. Comme R est ergodique, elle est nulle partout sauf sur l'un des ces atomes E , ce qui signifie que R est absolument continue par rapport à la restriction $\tilde{Q}_{|E}$. Deux mesures ergodiques distinctes ne peuvent avoir même support, donc à un coefficient près $R = \tilde{Q}_{|E}$.

b) Réciproquement la marginale $\tilde{Q}_{|E} \circ \eta^{-1}$ a son support contenu dans celui de Q , et comme il s'agit de deux mesures ergodiques, elles coïncident. $\tilde{Q}_{|E}$ est donc une solution de l'équation considérée.

2) La relation (2) résulte de la définition de d'' .

BIBLIOGRAPHIE

(1) BILLINGSLEY : "Ergodic Theory and Information". Wiley.

(2) BOË J.M. : "Représentations des monoïdes". Thèse de 3ème Cycle (1976).

(3) CLIFFORD A.H. and G.B. PRESTON : "The Algebraic Theory of Semigroups". Vol. 1 Amer. Math. Soc. (1961).

(4) DUVAL J.P. : "Périodes et répétitions des mots du monoïde libre". A paraître dans Theoretical Computer Science .

(5) EILENBERG S. : "Automata, Languages and Machines". Vol A, Academic Press (1974).

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