Ergod. Th. & Dynam. Sys. (1989), **9**, 469-477
Printed in Great Britain

Homomorphismes entre systèmes dynamiques définis par substitutions

B. HOST AND F. PARREAU

Département de Mathématiques, C.S.P. Université de Paris-Nord,
93430, *Villetaneuse, France*

(*Received* 30 *October* 1987)

Abstract. On étudie ici les homomorphismes métriques entre systèmes dynamiques définis par des substitutions de même longueur. En général, ces homomorphismes sont continus, et ont une forme simple. Le commutant essentiel d'un système dynamique défini par une substitution est fini, et peut être déterminé explicitement.

1. *Préliminaires et énoncé du résultat*

1.1. Les systèmes dynamiques définis par des substitutions ont été introduits par Gottschalk [2] et étudiés entre autres par Martin [4], Dekking [1] et Queffelec [5]. On rappelle dans ce paragraphe les définitions et les propriétés utilisées dans la suite; pour les démonstrations, on pourra se reporter à [6]. La seule notion nouvelle introduite ici est celle de substitution réduite.

Soit A un ensemble fini, appelé *alphabet*, dont les éléments sont appelés des *lettres.* Un *mot* sur A est une suite finie $\omega = (\omega_0, \ldots, \omega_k)$ de lettres; A^* désigne l'ensemble des mots sur $A \cdot q$ étant un entier > 1, une *substitution de longueur* q sur A est une application ξ de A dans A^* qui associe à chaque lettre un mot de longueur q. On étend par concaténation ξ en une application de A^* dans lui-même; cela permet d'itérer ξ: pour tout $n > 0$, ξ^n est une substitution de longueur q^n sur A. On dit qu'un mot ω sur A est *un mot de* ξ s'il existe une lettre a et un entier $n > 0$ tels que ω soit un sous-mot de $\xi^n a$. Si $x = (x_k; k \in \mathbb{Z})$ appartient à $A^{\mathbb{Z}}$ et si I est un intervalle de $\mathbb{Z}$, on note x_I le mot $(x_k; k \in I)$.

Soit X l'ensemble des suites $x \in A^{\mathbb{Z}}$ telles que, pour tout intervalle fini I de $\mathbb{Z}$, x_I soit un mot de $\xi \cdot X$ est une partie fermée de $A^{\mathbb{Z}}$, invariante par le 'shift' T de $A^{\mathbb{Z}}$. Le couple (X, T) sera appelé le système dynamique défini par ξ.

On s'intéresse ici uniquement aux substitutions ξ *primitives*, c'est à dire celles pour lesquelles il existe un entier $n > 0$ tel que pour tout couple (a, b) de lettres, b apparaît dans $\xi^n a$. Dans ce cas, le système dynamique topologique (X, T) admet une unique mesure de probabilité invariante μ. (X, T, μ) sera appelé le système dynamique métrique défini par ξ.

Par concaténation, on peut étendre ξ en une application de $A^{\mathbb{Z}}$ dans lui-même, encore notée ξ; il est clair que l'image de X par ξ est contenue dans X, et que ξ vérifie $\xi T = T^q \xi$.

ω et ω' étant deux mots de même longueur k, on note

$$d(\omega, \omega') = \frac{1}{k} \operatorname{card} \{j \in [0, k[;\ \omega_j \neq \omega'_j\}.$$

a et b étant deux lettres, la suite $(d(\xi^n a, \xi^n b))$ est décroissante. On dira que la substitution ξ est *réduite* si cette suite ne tend vers 0 que dans le cas où $a = b$. On verra plus loin (Proposition 1) que, si le système dynamique défini par ξ n'a pas un spectre purement discret, il est métriquement isomorphe au système dynamique défini par une substitution réduite canoniquement associé à ξ. Pour étudier les homomorphismes entre deux systèmes dynamiques définis par substitutions et dont le spectre n'est pas purement discret, on peut ainsi se ramener au cas où les substitutions sont réduites.

1.2. *Exemples d'homomorphismes.* A et B étant deux ensembles finis, et $k > 0$ un entier, on appelle *code de longueur k* une application U de $A^{\mathbf{Z}}$ dans $B^{\mathbf{Z}}$ commutant avec le shift et telle que, pour tout $x \in A^{\mathbf{Z}}$, $(Ux)_0$ ne dépende que de $x_{[0,k[}$. Soit $X \subset A^{\mathbf{Z}}$ un ensemble invariant par le shift, et $V : X \to B^{\mathbf{Z}}$; s'il existe un code $U : A^{\mathbf{Z}} \to B^{\mathbf{Z}}$ de longueur k dont la restriction à X soit égale à V, on dira encore que V est un code de longueur k.

(a) Soient ξ et ζ deux substitutions primitives de même longueur q sur les alphabets A et B, f une application de A dans B et $n > 0$ un entier tels que:

$$\text{pour tout } a \in A \text{ et tout } j \in [0, q^n[,\ (\zeta^n f(a))_j = f((\xi^n a)_j).$$

Soit U: $A^{\mathbf{Z}} \to B^{\mathbf{Z}}$ le code de longueur 1 défini par f. U vérifie $U\xi^n = \zeta^n U$. (X, T, μ) et (Y, T, ν) étant les systèmes dynamiques définis par ξ et ζ, UX est inclus dans Y; notons encore U la restriction de U à X. U est un homomorphisme de (X, T, μ) dans (Y, T, ν); un tel homomorphisme sera appelé un *homomorphisme trivial.* Lemanczyk et Mentzen [3] ont prouvé que tout isomorphisme entre deux systèmes dynamiques définis par des substitutions bijectives (cf § 3.1.) est le produit d'une puissance du shift et d'un homomorphisme trivial.

(b) Soit (X, T, μ) le système dynamique défini par une substitution primitive ξ de longueur q sur A. Soient B l'ensemble des mots de longueur 2 de ξ et $p \in [0, q-1[$. On définit une substitution ζ de longueur q sur B par:

$$(\zeta(a, b))_j = \begin{cases} ((\xi a)_{p+j}, (\xi a)_{p+j+1}) & \text{si } 0 \leq j < q-p-1; \\ ((\xi a)_{q-1}, (\xi b)_0) & \text{si } j = q-p-1; \\ ((\xi b)_{j+p-1}, (\xi b)_{j+p-q+1}) & \text{si } q-p \leq j < q. \end{cases}$$

La substitution ζ est primitive; soit (Y, T, ν) le système dynamique défini par ζ. L'application qui à chaque $(a, b) \in B$ associe a définit un code $U : B^{\mathbf{Z}} \to A^{\mathbf{Z}}$ de longueur 1. On vérifie facilement que $UY \subset X$; U est un isomorphisme de (Y, T, ν) sur (X, T, μ). L'isomorphisme U^{-1} de (X, T, μ) sur (Y, T, ν) est donné par un code de longueur 2. Il n'existe aucun entier n tel que $T^n U^{-1}$ soit trivial. Notons que $T^p U^{-1} \xi = \zeta U^{-1}$.

On peut généraliser cette construction en remplaçant la substitution ξ par une de ses itérées ξ^n et en choisissant l'entier p dans $[0, q^n - 1[$.

THÉORÈME 1.3. *Soient ξ et ζ deux substitutions primitives de même longueur q sur les alphabets A et B, et (X, T, μ) et (Y, T, ν) les systèmes dynamiques qu'elles définissent.*

https://doi.org/10.1017/S0143385700005113 Published online by Cambridge University Press

On suppose de plus que ζ est réduite et que Y est infini. Alors, pour tout homomorphisme S de (X, T, μ) dans (Y, T, ν), il existe un entier j tel que T^jS soit presque partout égal à un homomorphisme U vérifiant:

(1) *U est un code de longueur 2;*

(2) *il existe un entier $n>0$ et $p\in[0, q^n-1[$ avec $T^pU\xi^n=\zeta^nU$.*

REMARQUES. Tout homomorphisme S de (X, T, μ) dans (Y, T, ν) est donc presque partout égal à un homomorphisme continu; plus précisément, cet homomorphisme peut s'écrire comme un produit d'une puissance du shift, d'un homomorphisme trivial et d'un isomorphisme du type donné dans l'exemple (b).

Comme il n'existe qu'un nombre fini de codes de longueur 2, il n'existe, aux puissances du shift près, qu'un nombre fini d'homomorphismes de (X, T, μ) dans (Y, T, ν).

Remarquons enfin que la décomposition de S donnée dans le théorème est unique.

2. *Démonstration du théorème*

2.1. Y étant infini, on sait d'après [4] que la substitution ζ est 'déterminée', c'est à dire qu'il existe un entier $r>0$ tel que si $x\in\zeta Y$ et $y\in Y$ vérifient $x_{[-r,r]}=y_{[-r,r]}$, alors $y\in\zeta Y$. Dans toute la suite, r désignera un tel entier. Cette propriété signifie que ζY est une partie ouverte de Y, et que $\{T^k\zeta Y;\ 0\le k<q\}$ est une partition de Y. De même, pour toute $n>0$, ζ^nY est une partie ouverte de Y et $\{T^k\zeta^nY;\ 0\le k<q^n\}$ est une partition de Y. Pour toute $x\in Y$ et tout $n>0$, on notera $\pi_n(x)$ l'entier $k\in[0, q^n[$ tel que $x\in T^k\zeta^nY$. Remarquons que $\pi_{n+1}(x)=\pi_n(x)$ modulo q^n pour tout $n>0$ et tout $x\in Y$.

Par unique ergodicité, la mesure image de μ par S est ν, donc X est aussi infini, et on peut définir de même des applications de X dans $[0, q^n[$, que l'on notera aussi π_n.

Enfin, la propriété de partition que l'on vient de montrer, et l'unique ergodicité de (X, T) entraînent que la mesure image de μ par ξ^n est $q^n\cdot\mu|_{\xi^nX}$ (cf [6]); ainsi, pour tout borélien E de X,

$$\mu(E)=q^{-n}\int \operatorname{card}\{j\in[0, q^n[;\ T^j\xi^nx\in E\}\,d\mu(x).$$

Cette remarque servira plusieurs fois dans la suite.

On notera $\mathcal{H}$ l'ensemble des homomorphismes métriques de (X, T, μ) dans (Y, T, ν). Soient $W\in\mathcal{H}$ et $n>0$. L'application qui à tout $x\in X$ associe $\pi_n(x)-\pi_n(Wx)$ mod q^n est invariante par T donc presque partout égale à une constante que l'on notera $p_n(W)$. Ainsi, $T^{p_n(W)}W\xi^nX$ est inclus, à un ensemble négligeable près, dans ζ^nY; d'autre part, comme ζ est réduite, ζ^n est un homéomorphisme de Y sur ζ^nY; pour presque tout $x\in X$, il existe donc un unique $y\in Y$ tel que $T^{p_n(W)}W\xi^nx$ soit égal à ζ^ny; on notera W_nx cet élément y de Y. Comme $T^{q^n}\zeta^n=\zeta^nT$ et que $T^{q^n}\xi^n=\xi^nT$, $W_n\in\mathcal{H}$. On a ainsi associé, à chaque $W\in\mathcal{H}$, une suite $(p_n(W))$ d'entiers et une suite (W_n) dans $\mathcal{H}$ telles que, pour toute $n>0$

$$0\le p_n(W)<p^n \quad\text{et}\quad T^{p_n(W)}W\xi^n=\zeta^nW_n \text{ presque partout.}$$

On posera $p_0(W)=0$ et $W_0=W$. Remarquons que, pour tout $n\ge0$,

https://doi.org/10.1017/S0143385700005113 Published online by Cambridge University Press

$p_{n+1}(W) = p_n(W) + q^n p_1(W_n)$ et que $(W_n)_1 = W_{n+1}$; par récurrence, $(W_n)_j = W_{n+j}$ pour tous $n, j \geq 0$.

2.2. Comme ζ est réduite, il existe une constante $\eta > 0$ telle que $d(\zeta^n a, \zeta^n b) > \eta$ pour toutes lettres $a, b \in B$ distinctes et tout $n > 0$. Dans toute la suite, η désignera une telle constante.

Pour deux applications mesurables U et V de X dans $B^{\mathbf{Z}}$ commutant avec le shift, on note $d(U, V) = \mu\{x \in X; (Ux)_0 \neq (Vx)_0\}$.

LEMME 1. *Soient $U, V \in \mathscr{H}$. Si $d(U, V) < \eta/(2r+1)$, alors $U = V$ presque partout.*

Pour tout $n \geq 0$, notons $E_n = \{x \in X; (U_n x)_0 \neq (V_n x)_0\}$. Montrons par récurrence que $p_n(U) = p_n(V)$ et que $\mu(E_n) < 1/(2r+1)$ pour tout $n \geq 0$. Il n'y a rien à prouver pour $n = 0$. Soit $n > 0$, et supposons que ces propriétés sont vraies à l'ordre $n-1$. La fonction qui à tout $x \in X$ associe $\pi_1(U_{n-1}x) - \pi_1(V_{n-1}x)$ est égale presque partout à $p_1(V_{n-1}) - p_1(U_{n-1})$; par définition de r elle est nulle sur l'ensemble des $x \in X$ tels que $(U_{n-1}x)_{[-r,r]} = (V_{n-1}x)_{[-r,r]}$, et cet ensemble a une mesure >0 par hypothèse. Ainsi, $p_1(U_{n-1}) = P_1(V_{n-1})$, donc $p_n(U) = p_n(V)$. Notons $p = p_n(U)$. Pour tout $x \in E_n$, il existe au moins ηq^n entiers $k \in [0, q^n[$ tels que $(\zeta^n U_n x)_k \neq (\zeta^n V_n x)_k$, c'est à dire tels que $T^{p+k}\xi^n x \in E_0$. Ainsi,

$$\eta q^n \mu(E_n) \leq \int \operatorname{card}\{j \in [p, p+q^n[;\ T^j \xi^n x \in E_0\}\, d\mu(x)$$
$$= q^n \mu(E_0),$$

donc $\mu(E_n) < 1/(2r+1)$, et les propriétés annoncées sont vraies à l'ordre n.

Soit $k > 0$ un entier; choisissons un entier n tel que $q^n > 4k$, et posons $p = p_n(U)$. Si $x \in X$ vérifie $(U_n x)_0 = (V_n x)_0$, alors $(UT^{p+j}\xi^n x)_{[-k,k]} = (VT^{p+j}\xi^n x)_{[-k,k]}$ pour tout $j \in [k, q^n - k]$. Ainsi

$$\mu\{x \in X; (Ux)_{[-k,k]} = (Vx)_{[-k,k]}\} \geq (1 - 2kq^{-n})\mu(X \setminus E_n)$$
$$\geq r/(2r+1).$$

L'ensemble des $x \in X$ tels que $Ux = Vx$ est l'intersection décroissante de ces ensembles pour $k \in \mathbb{N}$, il a donc une mesure >0. Par ergodicité, $U = V$ presque partout.

2.3.

LEMME 2. *Soit $S \in \mathscr{H}$. Il existe une suite (f_n) de codes de longueur 2 telle que $d(S_n, f_n)$ tende vers 0.*

Soit $\varepsilon > 0$. S étant mesurable, il existe un entier $m > 0$ et une application g de X dans B telle que $g(x)$ ne dépende que de $x_{[-m,m]}$ et que l'ensemble $E = \{x \in X; (Sx)_0 \neq g(x)\}$ ait une mesure inférieure à $\varepsilon\eta/6$. Choisissons n assez grand pour que $m < \eta q^n/6$, et posons $p = p_n(S)$. Pour tout $x \in X$, notons $\Lambda(x)$ l'ensemble des entiers $k \in [m, q^n - m]$ tels que $T^{k+p}\xi^n x$ n'appartienne pas à E. Soit enfin $F = \{x \in X; \operatorname{card} \Lambda(x) > (1 - \eta/2)q^n\}$.

Montrons que S_n coïncide sur F avec un code de longueur 2. Soient $x, y \in F$ avec $x_{[0,1]} = y_{[0,1]}$. Pour tout $k \in [m, q^n - m]$, $(T^{p+k}\xi^n x)_{[-m,m]} = (T^{p+k}\xi^n y)_{[-m,m]}$, donc $g(T^{p+k}\xi^n x) = g(T^{p+k}\xi^n y)$. Si $k \in \Lambda(x) \cap \Lambda(y)$, $(\zeta^n S_n x)_k = g(T^{p+k}\xi^n x) =$

https://doi.org/10.1017/S0143385700005113 Published online by Cambridge University Press

$g(T^{p+k}\xi^n y) = (\zeta^n S_n y)_k$. Enfin, comme x et y appartiennent à F, card $(\Lambda(x) \cap \Lambda(y)) > (1-\eta)q^n$, donc $(S_n x)_0 = (S_n y)_0$ par définition de η. Ainsi, pour $x \in F$, $(S_n x)_0$ ne dépend que de $x_{[0,1]}$. D'autre part,

$$\varepsilon\eta/6 > \mu(E) \geq q^{-n} \int (q^n - 2m - \text{card } \Lambda(x))\, d\mu(x)$$

$$\geq (1-\mu(F))\eta/6,$$

donc $\mu(F) > 1-\varepsilon$, d'où le résultat.

Remarque. On n'a pas prouvé que $f_n(X)$ est inclus dans Y, c'est à dire que f_n est un homomorphisme; on ne peut donc pas appliquer directement le lemme 1 à S_n et f_n.

COROLLAIRE 1. *Soit $S \in \mathcal{H}$. S'il existe $n > 0$ tel que $S = S_n$ presque partout, alors S est presque partout égal à un code de longueur* 2. *En particulier, la propriété* 2 *du théorème implique la propriété* 1.

Pour tout $j \geq 0$, $S_{n+j} = (S_n)_j = S_j$; en particulier $S_{2n} = S_n$ et, par récurrence, $S_{kn} = S$ pour tout $k \geq 0$. Comme il n'existe qu'un nombre fini de codes de longueur 2, le Lemme 2 entraîne que S est un code de longueur 2.

Remarque. Sous les mêmes hypothèses, S_j est un code de longueur 2 pour tout $j \geq 0$; on peut en déduire que l'entier n peut être choisi inférieur ou égal au nombre de codes de longueur 2.

2.4. *Fin de la démonstration du théorème.* A et B étant finis, il n'existe qu'un nombre fini de codes de longueur 2. D'après le Lemme 2, il existe donc deux entiers $m \geq 0$ et $k > 0$ tels que $d(S_m, S_{m+k}) < \eta/(2r+1)$. D'après le lemme 1, $S_m = S_{m+k}$.

Soit $n \geq m$ un entier multiple de k; posons $U = S_n$, $p = p_n(U)$ et $j = p_n(S) - p$. Alors $U_k = (S_n)_k = S_{n+k} = (S_{m+k})_{n-m} = (S_m)_{n-m} = S_n = U$; par récurrence, $U_{rk} = U$ pour tout $r > 0$; comme n est un multiple de k, $U_n = U$. D'après le corollaire, U est un code de longueur 2. Par définition de p, $T^p U \xi^n = \zeta^n U$. D'autre part, $T^j S \xi^n = T^{-p}\zeta^n U = U\xi^n$; $T^j S$ et U coïncident presque partout sur $\xi^n X$ donc presque partout sur X par ergodicité.

On a bien écrit S sous la forme annoncée. Il reste à éliminer le cas où $p = q^n - 1$. Dans ce cas, posons $V = T^{j-1} S$. V vérifie $V\xi^n = \zeta^n V$, donc V est un code de longueur 2 d'après le Corollaire 1; on s'est ainsi ramené au cas où $p = 0$, ce qui achève la démonstration.

3. *Cas particuliers*

3.1. *On conserve les notations du théorème.* Soit $\mathcal{D}$ l'ensemble des homomorphismes U pour lesquels il existe $n > 0$ avec $U = U_n$, c'est à dire:

$$\text{il existe } p \in [0, q^n - 1[\text{ avec } T^p U \xi^n = \zeta^n U.$$

D'après le Corollaire 1, tout homomorphisme $U \in \mathcal{D}$ est un code de longueur 2. On peut dans certains cas préciser ce résultat et montrer que U est un code de longueur 1, ou même un homomorphisme trivial.

https://doi.org/10.1017/S0143385700005113 Published online by Cambridge University Press

Soit $U \in \mathscr{D}$. Quitte à remplacer ξ par ξ^n, ζ par ζ^n et q par q^n, on peut se ramener au cas où $U = U_1$, c'est à dire supposer qu'il existe $p \in [0, q-1[$ avec $T^p U\xi = \zeta U$.

LEMME 3. *Soient $U \in \mathscr{D}$ et $p \in [0, q-1[$ avec $T^p U\xi = \zeta U$. Si $p < \eta(q-1)$, alors U est un code de longueur* 1; *en particulier, si $p = 0$, U est trivial. Si $p > (1-\eta)(q-1)$, alors $T^{-1}U$ est un code de longueur* 1.

Supposons que $p < \eta(q-1)$; soit $k > 0$ tel que l'entier $s = p(q^k - 1)/(q-1)$ soit strictement inférieur à $\eta q^k - 1$. Comme $T^s U\xi^k = \zeta^k U$, pour $x \in X$ la donnée de x_0 détermine $(\zeta^k Ux)_{[0, q^k-2-s]}$ donc $(Ux)_0$ car $q^k - 1 - s > (1-\eta)q^k$; U est donc un code de longueur 1. Si $p = 0$, l'application $f : A \to B$ définie par $(Ux)_0 = f(x_0)$ pour tout $x \in X$ vérifie $(\zeta f(a))_j = f((\xi a)_j)$ pour tout $a \in A$ et tout $j \in [0, q[$, donc U est trivial. La deuxième partie du lemme se montre de la même façon.

Le lemme précédent s'applique en particulier si la substitution ζ est *bijective*, c'est à dire si, pour tout $j \in [0, q[$, les lettres $((\zeta a)_j ; a \in B)$ sont toutes distinctes; dans ce cas ζ est réduite, et sa constante η est 1.

COROLLAIRE 2. *Si les substitutions ξ et ζ sont bijectives, tout homomorphisme $U \in \mathscr{D}$ est trivial. Tout homomorphisme entre les systèmes définis par ξ et ζ est le produit d'une puissance du shift et d'un homomorphisme trivial.*

Soient $u \in \mathscr{D}$ et $p \in [0, q-1[$ avec $T^p U\xi = \zeta U$. Il suffit de montrer que $p = 0$; supposons que p n'est pas nul. D'après le Lemme 3, il existe deux applications f et g de A dans B telles que, pour tout $x \in X$, $(Ux)_0 = f(x_0) = g(x_1)$.

Soient a, $a' \in A$. ξ étant bijective, il existe b, $b' \in A$ telles que $(\xi b)_{q-1} = a$ et $(\xi b')_{q-1} = a'$. De la relation de commutation vérifiée par U, on déduit facilement que $f(a) = (\zeta f(b))_{q-1-p}$, que $g(a) = (\zeta f(b))_{q-2-p}$ et les mêmes relations avec a' et b' à la place de a et b. La substitution ζ étant bijective, on a alors

$$f(a) = f(a') \quad \Leftrightarrow \quad f(b) = f(b') \quad \Leftrightarrow \quad g(a) = g(a').$$

Soient maintenant y, $y' \in Y$ avec $y_0 = y'_0$. Par minimalité, il existe x, $x' \in X$ tels que $Ux = y$ et $Ux' = y'$. On a alors $f(x_0) = f(x'_0)$ donc $g(x_0) = g(x'_0)$ et $y_{-1} = y'_{-1}$; de même, $y_1 = y'_1$ et par récurrence $y = y'$. Y est donc fini, d'où une contradiction.

3.2. *Commutant.* Soit (X, T, μ) le système dynamique défini par la substitution primitive ξ de longueur q sur l'alphabet A; on suppose que ξ est réduite et que X est infini. Il est classique que le commutant $\mathscr{G}$ de ce système est un groupe (car (X, T, μ) est une extension finie d'un système à spectre purement discret). D'après le théorème, le commutant essentiel, quotient de $\mathscr{G}$ par le sous-groupe $\{T^j ; j \in \mathbb{Z}\}$ est fini; chaque élément du commutant essentiel est représenté par un automorphisme appartenant à l'ensemble $\mathscr{D}$ défini au paragraphe précédent.

Si $U \in \mathscr{D}$ vérifie $T^p U\xi^n = \xi^n U$, alors, tout $k > 0$, U vérifie aussi $T^m U\xi^{nk} = \xi^{nk} U$ avec $m = p(q^{nk} - 1)/(q^n - 1)$; comme $\mathscr{D}$ est fini, il existe un entier $n > 0$ tel que, pour tout $U \in \mathscr{D}$, il existe $p \in [0, q^n - 1[$ avec $T^p U\xi^n = \xi^n U$; quitte à remplacer ξ par ξ^n et q par q^n on peut supposer que $n = 1$. Ainsi, pour tout $U \in \mathscr{D}$, il existe un entier $p(U) \in [0, q-1[$ avec $T^{p(U)} U\xi = \xi U$.

https://doi.org/10.1017/S0143385700005113 Published online by Cambridge University Press

Soient U et $V \in \mathscr{D}$. Si $p(U)+p(V) < q-1$, alors $UV \in \mathscr{D}$ et $p(UV) = p(U)+p(V)$; si $p(U)+p(V) \geq q-1$, alors $T^{-1}UV$ appartient à $\mathscr{D}$ et $p(T^{-1}UV) = p(U)+p(V)-q+1$. Ainsi, $\{p(U) \bmod q-1;\ U \in \mathscr{D}\}$ est un sous-groupe de $\mathbb{Z}/(q-1)\mathbb{Z}$. Il y a deux cas possibles:

- Ou bien tout $U \in \mathscr{D}$ est trivial, et le commutant est $\{T^jS;\ j \in \mathbb{Z},\ S \text{ trivial}\}$.
- Sinon, il existe un entier $m > 1$ divisant $(q-1)$ et $U \in \mathscr{D}$ tels que $p(U) = (q-1)/m$, et tel que $T^{-1}U^m$ soit trivial; le commutant est alors $\{T^jUS^k;\ j \in \mathbb{Z},\ 0 \leq k < m,\ S \text{ trivial}\}$. Du Lemme 3, on déduit facilement que $m \leq 1/\eta$.

3.3. *Existence d'une racine carrée du shift.* On conserve ici les hypothèses du paragraphe précédent. On donne un algorithme permettant de déterminer si T admet une racine carrée. Supposons d'abord que T admette une racine carrée S.

Soient $j \in \mathbb{Z}$ tel que $U = T^jS$ appartienne à $\mathscr{D}$, $n > 0$ et $p \in [0, q^n - 1[$ tels que $T^pU\xi^n = \xi^nU$. Comme $U^2 = T^{2j+1}$, un calcul immédiat montre que $j = 0$ et que $p = (q^n-1)/2$. Ainsi, q est impair, l'entier m introduit au paragraphe précédent est pair, S appartient à $\mathscr{D}$ et il existe $n > 0$ avec $T^{(q^n-1)/2}S\xi^n = \xi^nS$.

Il est immédiat que, pour tout $j \geq 0$, $p_j(S) = (q^j-1)/2$, $S_j^2 = T$ et S_j est le produit de S et d'un automorphisme trivial; on peut en déduire que l'entier n peut être choisi inférieur ou égal au nombre t d'automorphismes triviaux.

D'autre part, S est un code de longueur 2; il est donnè par une application $f: A^2 \to A$; pour un certain $n \leq t$, en posant $p = (q^n-1)/2$, f vérifie:

$$(\xi^n f(a,b))_j = \begin{cases} f((\xi^n a)_{j+p}, (\xi^n a)_{j+p+1}) & \text{si } 0 \leq j < q^n - 1 - p, \\ f((\xi^n a)_{q^n-1}, (\xi^n b)_0) & \text{si } j = q^n - 1 - p, \\ f((\xi^n b)_{j-q^n+p}, (\xi^n b)_{j-q^n+p+1}) & \text{si } q^n - p \leq j \leq q^n - 1. \end{cases} \tag{1}$$

pour tout mot (a, b) de longueur 2 de ξ. Comme $s^2 = T$, f vérifie d'autre part

$$f(f(a,b), f(b,c)) = b \tag{2}$$

pour tout mot (a, b, c) de longueur 3 de ξ.

Réciproquement, soit $f: A^2 \to A$ satisfaisant (1) et (2), et soit $S: A^{\mathbf{Z}} \to B^{\mathbf{Z}}$ le code de longueur 2 définit par f; la relation (1) entraîne que $S(X)$ est inclus dans X donc que S est un automorphisme de (X, T, μ); la relation (2) entraîne que $S^2 = T$. On peut ainsi déterminer si T a une racine carrée en nombre fini d'étapes.

3.4. *Un exemple.* Soient $A = \{a, a', b, b'\}$ et ξ la substitution de longueur 3 sur A donnée par:

$$\xi a = ab'b; \quad \xi a' = a'bb'; \quad \xi b = aa'b'; \quad \xi b' = a'ab.$$

Cette substitution est primitive et réduite avec une constante $\eta = \frac{1}{2}$; elle définit un système dynamique (X, T, μ) infini. Ce système possède deux automorphismes triviaux: l'identité I et le code S de longueur 1 qui échange d'une part a et a' et d'autre part b et b'. Soit U le code de longueur 2 vérifiant $US = SU$ et donné par:

$$aa \to a; \quad aa' \to b; \quad ab \to a; \quad ab' \to b;$$
$$ba \to b'; \quad ba' \to a'; \quad bb \to b'; \quad bb' \to a'.$$

Un calcul simple montre que $TU\xi = \xi U$, et on en déduit que l'image de X par U est contenue dans X: X est un automorphisme de (X, T, μ); U est une racine carrée

de T. D'après le § 3.2., les automorphismes de ce système sont tous de la forme T^jW, où $j \in \mathbb{Z}$ et $W \in \{I, S, U, SU\}$.

Comme $U^2 = T$, $U^3\xi = \xi U$. En fait, on peut montrer que le système (X, U, μ) est isomorphe au système défini par une substitution: soient $B = \{0, 1\}$, ζ la substitution sur B donnée par $\zeta 0 = 001$ et $\zeta 1 = 110$, et (Y, T, ν) le système dynamique qu'elle définit. le code de longueur 2 donné par:

$$00 \to a; \quad 01 \to b; \quad 10 \to b'; \quad 11 \to a'$$

est un isomorphisme de (Y, T, ν) sur (X, U, μ); cette remarque s'étend au cas général.

4. *Réduction des substitutions*

On montre ici le résultat annoncé au § 1.1. Soit ξ une substitution de longueur q sur A. On dit que deux lettres a et b sont *équivalentes*, et on note $a \sim b$, si $d(\xi^n a, \xi^n b) \to 0$ quand $n \to +\infty$; l'aphabet réduit $\tilde{A}$ est le quotient de A par cette relation d'équivalence; la classe d'un lettre $a \in A$ est notée $\tilde{a}$. Si deux lettres a et b sont équivalentes, alors $(\xi a)_j \sim (\xi b)_j$ pour tout $j \in [0, q[$; on peut donc définir une substitution $\tilde{\xi}$ sur $\tilde{A}$ par $(\tilde{\xi}\tilde{a})_j = ((\xi a)_j)^{\sim}$ pour $0 \leq j < q$. Cette substitution est réduite; on l'appelle la *substitution réduite de* ξ.

Pour $x \in A^{\mathbb{Z}}$, on note $\tilde{x}$ l'élément $(\tilde{x}_j; j \in Z)$ de $\tilde{A}^{\mathbb{Z}}$. L'application $x \to \tilde{x}$ est un homomorphisme du système dynamique défini par ξ sur le système dynamique défini par $\tilde{\xi}$.

PROPOSITION 1. *Soient (X, T, μ) le système dynamique défini par une substitution ξ de longueur q sur A, et $(\tilde{X}, T, \tilde{\mu})$ le système dynamique défini par la substitution réduite $\tilde{\xi}$ de ξ. Si (X, T, μ) n'a pas un spectre purement discret, l'homomorphisme naturel de ce système sur $(\tilde{X}, T, \tilde{\mu})$ est un isomorphisme métrique.*

Comme (X, T, μ) n'a pas un spectre purement discret, on déduit facilement des résultats de [1] que $\tilde{X}$ est infini; on peut donc définir des applications $\pi_n : \tilde{X} \to [0, q^n[$ comme au § 2.1. L'homomorphisme naturel de X dans $\tilde{X}$ est trivial: $\pi_n(x) = \pi_n(\tilde{x})$ pour tout n et tout $x \in X$; en particulier, si $x, y \in X$ vérifient $\tilde{x} = \tilde{y}$, alors $\pi_n(x) = \pi_n(y)$ pour tout n.

Soit E l'ensemble des $x \in X$ pour lesquels il existe $y \in X$ avec $\tilde{x} = \tilde{y}$ et $x_0 \neq y_0$. Il suffit de montrer que $\mu(E) = 0$.

Soient $n > 0$, $j \in [0, q^n[$ et $x \in X$ tels que $T^j\xi^n x \in E$. Il existe $y \in X$ avec $(T^j\xi^n x)^{\sim} = \tilde{y}$ et $y_0 \neq (\xi^n x_0)_j$. D'après ce qui précède, $\pi_n(y) = \pi_n(T^j\xi^n x) = j$ et il existe $z \in X$ avec $y = T^j\xi^n z$. Ainsi, $(T^j\xi^n z)^{\sim} = (T^j\xi^n x)^{\sim}$ et en particulier $(\xi^n z_0)_j \sim (\xi^n x_0)_j$; d'autre part, $(\xi^n z_0)_j = y_0 \neq (\xi^n x_0)_j$; l'entier j appartient donc à l'ensemble Σ_n donné par:

$$\Sigma_n = \bigcup_{a,b \in A} \{j \in [0, q^n[; (\xi^n a)_j \sim (\xi^n b)_j \text{ et } (\xi^n a)_j \neq (\xi^n b)_j\}.$$

On a donc:

$$\mu(E) = q^{-n} \int \operatorname{card}\{j \in [0, q^n[; T^j\xi^n x \in E\}\, d\mu(x)$$

$$\leq q^{-n} \operatorname{card} \Sigma_n.$$

https://doi.org/10.1017/S0143385700005113 Published online by Cambridge University Press

Or, pour tout $n > 0$,

$$q^{-n} \operatorname{card} \Sigma_n \leq \sum_{a,b \in A} \left(d(\xi^n a, \xi^n b) - \lim_{k \to \infty} d(\xi^k a, \xi^k b) \right),$$

donc $q^{-n} \operatorname{card} \Sigma_n$ tend vers 0 quand $n \to +\infty$, et $\mu(E) = 0$, ce qu'il fallait démontrer.

REFERENCES

[1] F. M. Dekking. The spectrum of dynamical systems arising from substitutions of constant length. *Z. Wahr. Verw. Geb.* **41** (1978), 221-239.

[2] W. H. Gottschalk. Substitution minimal sets. *Trans. Amer. Math. Soc.* **109** (1963), 467-491.

[3] M. Lemanczyk & M. K. Mentzen. On metric properties of bijective substitutions. À paraître.

[4] J. C. Martin. Substitution minimal flows. *Amer. J. Math.* **93** (1971), 503-526.

[5] M. Queffelec. Contribution à l'étude spectrale des suites arithmétiques, Thèse. Université de Paris Nord (1984).

[6] M. Queffelec. Substitutions dynamical systems. Spectral analysis. *Lecture Notes in Mathematics* **1294** (Springer Verlag, Berlin, 1987).