COMPOSITIO MATHEMATICA

CHRISTIAN MAUDUIT
BRIGITTE MOSSÉ

Étude spectrale de la multiplication q-adique

Compositio Mathematica, tome 67, nº 2 (1988), p. 129-147
<http://www.numdam.org/item?id=CM_1988__67_2_129_0>

Compositio Mathematica 67: 129–147 (1988)

Etude spectrale de la multiplication q-adique

CHRISTIAN MAUDUIT[1] & BRIGITTE MOSSÉ[2]
[1] *UA 225 CNRS, Université d'Aix-Marseille II, Département de Mathématique-Informatique, 70, route Léon Lachamp, 13288 Marseille Cedex 9, France;* [2] *UA 225 CNRS, Université de Provence, Département de Mathématiques, 3, place Victor-Hugo, 13331 Marseille Cedex 3, France*

Received 19 June 1987; accepted in revised form 8 January 1988

Résumé. q désignant un nombre premier et k un entier naturel, nous étudions l'ensemble des multiples de k au sens de la multiplication q-adique, induite sur $\mathbb{N}$ par la multiplication dans $\mathbb{F}_q[X]$. Nous présentons parallèlement l'étude spectrale classique et l'étude spectrale q-adique de ces ensembles.

Abstract. Let q be a prime number and k a natural integer. We develop a classical and a q-adic spectral study of the set of the q-adic multiples of k.

I. Introduction et définitions

L'analyse spectrale des suites a fait récemment l'objet de nombreux travaux, en particulier dans le cas des suites arithmétiques dont la définition est liée à la donnée d'une base q (cf. [1, 2, 4–8, 12, 14]). Parallèlement, l'étude spectrale q-adique présentée dans [3, 11] adapte les outils habituels à ce genre de suites. Son intérêt, dans le cas des suites q-multiplicatives, a été développé dans [12]: par exemple, on associe à une suite q-multiplicative une mesure spectrale q-adique, qui s'exprime sous forme d'un produit de convolution aux propriétés de pureté remarquables. Nous étudions ici le cas, en général non q-multiplicatif, de l'ensemble des multiples d'un entier au sens de la multiplication q-adique, induite sur $\mathbb{N}$ par la multiplication dans $\mathbb{F}_q[X]$ (dans tout ce qui suit, q désigne un nombre premier).

1. Opérations induites sur $\mathbb{N}$ par $\mathbb{F}_q[X]$

A tout entier naturel n, qui s'écrit de façon unique sous la forme $n = \Sigma_{r\geqslant 0}\, p_r(n)q^r$ (avec, pour tout entier r, $p_r(n) \in \{0, \ldots, q-1\}$), on associe l'élément de $\mathbb{F}_q[X]$:

$$P_n(X) = \sum_{r\geqslant 0} \dot{p}_r(n)X^r,$$

où l'on désigne par $\dot{a}$ la classe modulo q d'un entier a.

Travail effectué dan le cadre du PRC "Arithmétique, langages et Informatique théorique".

D'autre part, nous pouvons associer à tout élément $P(X)$ de $\mathbb{F}_q[X]$ son image par l'injection canonique dans $\mathbb{Z}[X]$, notée $\tilde{P}(X)$. Les opérations induites sur $\mathbb{N}$ par $\mathbb{F}_q[X]$, appelées addition et multiplication q-adiques, sont alors définies de la manière suivante:

$$n \oplus n' = (\widetilde{P_n + P_{n'}})(q) \quad \text{et} \quad n \otimes n' = (\widetilde{P_n \cdot P_{n'}})(q).$$

On notera A_q l'anneau $(\mathbb{N}, \oplus, \otimes)$ et G_q le groupe $(\mathbb{N}, \oplus)$.

2. Ensemble reconnu par un q-automate

Un q-automate $\mathscr{A}$ est la donnée d'un quintuplet (E, F, e, φ, τ) où E et F sont deux ensembles finis, e un élément de E (appelé état initial), φ une application de $E \times \{0, \ldots, q-1\}$ vers E et τ une application de E vers F.

Pour tout (x, a) dans $E \times \{0, \ldots, q-1\}$ on pose $\varphi(x, a) = x \cdot a$ et on prolonge φ en une application de $E \times \mathbb{N}$ vers E, encore notée φ, de la façon suivante: si n est un entier naturel dont la représentation en base q est

$$p_g(n)p_{g-1}(n) \ldots p_0(n),$$

on pose pour tout x dans E:

$$\begin{aligned} \varphi(x, n) &= x \cdot n \\ &= (\ldots (x \cdot p_g(n))p_{g-1}(n) \ldots)p_0(n). \end{aligned}$$

DÉFINITION 1. On dit qu'une suite $u \in F^{\mathbb{N}}$ est q-reconnaissable s'il existe un q-automate $\mathscr{A} = (E, F, e, \varphi, \tau)$ tel que:

$$u = (\tau \circ \varphi(e, n))_{n \in \mathbb{N}}.$$

DÉFINITION 2. On dit qu'une partie de $\mathbb{N}$ est q-reconnaissable si sa fonction indicatrice $u \in \{0, 1\}^{\mathbb{N}}$ est q-reconnaissable.

L'anneau A_q étant principal, ses idéaux sont de la forme $\mathfrak{J}_q(k) = \{k \otimes n, n \in \mathbb{N}\}$ où k est un entier naturel. Nous montrons (cf. théorème 1) que les éléments de $\mathfrak{J}_q(k)$ peuvent être caractérisés par une propriété simple de leur développement q-adique, et sont ainsi reconnus par un q-automate.

3. Rappels d'analyse spectrale

(*a*) *Analyse spectrale classique* (cf. [15])
On note $\mathscr{S}$ l'espace de Wiener des suites u à valeurs dans $\mathbb{U} = \{z \in \mathbb{C}; |z| = 1\}$ telles que

$$u_0 = 1 \quad \text{et} \quad \lim_{N \to +\infty} \frac{1}{N} \sum_{n<N} u_{n+t} \overline{u_n}$$

existe pour tout entier positif t. Pour tout $t \in \mathbb{N}$, on pose

$$\gamma(t) = \lim_{N \to +\infty} \frac{1}{N} \sum_{n<N} u_{n+t} \overline{u_n} \quad \text{et} \quad \gamma(-t) = \overline{\gamma(t)}.$$

γ est appelée corrélation de la suite u. La suite γ, définie positive, est la transformée de Fourier d'une mesure borélienne de probabilité sur $\mathbb{U}$ appelée mesure spectrale de u. T désignant le décalage défini sur $\mathbb{U}^{\mathbb{N}}$, qui à $u = (u_i)_{i \in \mathbb{N}}$ associe $T \cdot u = (u_{i+1})_{i \in \mathbb{N}}$, on note K_u la fermeture de l'orbite de u sous l'action de T dans $\mathbb{U}^{\mathbb{N}}$, et μ une valeur d'adhérence de la suite

$$\left(\frac{1}{N} \sum_{n<N} \delta_{T^n . u} \right)_{N \in \mathbb{N}^*}.$$

A tout élément f de $L^2(K_u, \mu)$-normalisé par les conditions $\|f\|_2 = 1$ et $f \perp \mathbb{C}$, nous associons alors plus généralement une mesure λ_f dont la transformée de Fourier est la corrélation γ_f de f, définie par:

$$\forall n \in \mathbb{N} \ \gamma_f(n) = \int_{K_u} f \circ T^n . \bar{f} \, \mathrm{d}\mu \quad \text{et} \quad \gamma_f(-n) = \overline{\gamma_f(n)}.$$

On a $\gamma = \gamma_{p_0}$, où p_0 est la restriction à K_u de la première projection de $\mathbb{U}^{\mathbb{N}}$.

Dans le cas où μ est uniquement déterminée, on note σ_m le type spectral maximal de u, c'est-à-dire la classe d'une mesure λ_f dominante. On dit que u est à spectre singulier (resp. discret, de Lebesque, . . .) si σ_m est singulière (resp. discrète, de Lebesgue, . . .). De plus, on dit que u est à spectre simple s'il existe g dans $L^2(K_u, \mu)$ tel que le sous-espace engendré par $\{g \circ T^n, n \in \mathbb{N}\}$ est dense dans $L^2(K_u, \mu)$.

(*b*) *Analyse spectrale q-adique* (cf. [11])
De manière analogue, on définit (cf. [3, 11]) l'espace $\mathscr{S}_q$ des suites u à valeurs dans $\mathbb{U}$ telles que $u_0 = 1$ et

$$\gamma_q(t) = \lim_{N \to +\infty} \frac{1}{N} \sum_{n<N} u_{n \oplus t} \overline{u_n}$$

existe pour tout $t \in \mathbb{N}$. $\gamma_q = (\gamma_q(t))_{t\in\mathbb{N}}$ est appelée corrélation de Walsh de u. Le dual $\hat{G}_q$ étant isomorphe à $\mathbb{F}_q^{\mathbb{N}}$, on définit pour tout $n \in \mathbb{N}$:

$$w_n\colon \hat{G}_q \to \mathbb{U}$$

$$x = (\dot{x}_r)_{r\in\mathbb{N}} \to w_n(x) = \prod_{r\geqslant 0} \mathrm{e}\,(p_r(n)x_r/q)$$

(en posant $\mathrm{e}(z) = \mathrm{e}^{2i\pi z}$).

$(w_n)_{n\in\mathbb{N}}$ est une base de caractères de $\hat{G}_q$, appelés caractères de Walsh. γ_q étant G_q-définie positive, elle est la transformée de Fourier–Walsh d'une mesure borélienne de probabilité sur $\hat{G}_q$, appelée mesure spectrale de Walsh de u.

T_n désignant, pour tout entier naturel n, le décalage q-adique défini sur $\mathbb{U}^{\mathbb{N}}$, qui à $u = (u_i)_{i\in\mathbb{N}}$ associe $T_n . u = (u_{i\oplus n})_{i\in\mathbb{N}}$, on note comme précédemment K_u^q la fermeture de l'orbite de u sous l'action de u sous l'action de G_q, et μ_q une valeur d'adhérence de la suite

$$\left(\frac{1}{N}\sum_{n<N}\delta_{T_n.u}\right)_{N\in\mathbb{N}^*}.$$

A tout élément normalisé f de $L^2(K_u^q, \mu_q)$ ($\|f\|_2 = 1$ et $f \perp \mathbb{C}$), nous associons une mesure λ_f^q dont la transformée de Fourier–Walsh est la corrélation de f, définie par:

$$\forall n \in \mathbb{N},\ \gamma_f^q(n) = \int_{K_u^q} f\circ T_n . \bar{f}\,\mathrm{d}\mu_q.$$

On a ainsi $\gamma_q = \gamma_{p_0}^q$, où p_0 est la restriction à K_u^q de la première projection de $\mathbb{U}^{\mathbb{N}}$. On note σ_m^q le type spectral maximal de Walsh de u, défini de manière analogue à σ_m.

A l'idéal de A_q engendré par k est associée, de manière naturelle, une suite u à valeurs dans $\mathbb{U}$, dont nous montrons que le spectre de Walsh est discret (cf. théorème 3).

Par ailleurs, nous précisons le support de la composante discrète de σ_m, et nous montrons que le spectre de u est simple et singulier (cf. théorème 4).

II. Propriétés élémentaires des idéaux de A_q

1. Caractère automatique

Proposition 1. *Soit k un entier naturel.*
Il existe $(d, d', \ell) \in \mathbb{N}^3$ et, pour tout $(i, b) \in \{1, \ldots, d\} \times \{0, \ldots, \ell - 1\}$, il existe $\lambda(i, b) \in (0, \ldots, q - 1\}$ tel que $\mathcal{T}_q(k)$ soit égal à l'ensemble des

entiers $n = \Sigma_{r \geqslant 0} p_r(n) q^r$ *qui vérifient les d égalités*

$$\mathrm{i} \in \{1, \ldots, d\} \quad \sum_{a \geqslant 0} \sum_{b < \ell} \lambda(i, b) p_{a\ell + b}(n) = 0 \bmod \cdot q$$

et les d égalités

$$p_0(n) = \cdots = p_{d'-1}(n) = 0.$$

DÉMONSTRATION Un entier n est multiple dans A_q de k si et seulement si P_k divise P_n dans $\mathbb{F}_q[X]$. Soit $\mathbb{F}$ le corps de décomposition de P_k sur $\mathbb{F}_q$. P_k se factorise sur $\mathbb{F}[X]$ en

$$P_k(X) = \lambda \prod_{i < s} (X - \alpha_i)^{m_i}$$

où les α_i sont les racines de P_k dans $\mathbb{F}$, de multiplicité $m_i > 0$. Soit α l'une de ces racines et m sa multiplicité.

- Si α est nul, $P_n(X)$ est multiple de $(X - \alpha)^m$ si et seulement si $p_0(n) = \cdots = p_{m-1}(n) = 0$.

- Si α est non nul, $\mathbb{F}$ étant fini, α est racine de l'unité: soit w son ordre et soit δ le degré de son polynôme minimal sur $\mathbb{F}_q$. Si $P(X) = \Sigma_{r \geqslant 0} p_r X^r \in \mathbb{F}_q[X]$, l'égalité $P(\alpha) = 0$ équivaut à δ égalités de la forme

$$(*) \sum_{a \geqslant 0} \sum_{b < w} \lambda_{i,b} p_{aw+b} = 0 \quad (i \in \{0, \ldots, \delta - 1\}),$$

les $\lambda_{i,b}$ étant les éléments de $\mathbb{F}_q$ déterminés par les égalités:

$$\alpha^b = \sum_{i=0}^{\delta - 1} \lambda_{i,b} \alpha^i.$$

Soit alors $(P_n^{[j]})_{j \in \mathbb{N}}$ la suite d'éléments de $\mathbb{F}_q[X]$ définis par:

$$P_n(X + Y) = \sum_{j \geqslant 0} P_n^{[j]}(X) Y^j.$$

On a, pour tout $j \in \{0, \ldots, m - 1\}$,

$$P_n^{[j]}(X) = \sum_{r \geqslant 0} p_{r+j}(n) \binom{r + j}{j} X^r.$$

$P_n(X)$ est un multiple de $(X - \alpha)^m$ si et seulement si

$$P_n^{[0]}(\alpha) = P_n^{[1]}(\alpha) = \cdots = P_n^{[m-1]}(\alpha) = 0.$$

On conclut en écrivant successivement les égalités (*) pour $P = P_n^{[0]}, \ldots, P_n^{[m-1]}$ et en remarquant que pour tout j, la suite $(\binom{n}{j})_{n \in \mathbb{N}}$ est périodique, de période q^h si $q^h \geqslant j$ (en effet, $\forall n \in \mathbb{N}$ $(X+1)^{n+q^h} = (X+1)^n(X^{q^h}+1)$ dans $\mathbb{F}_q[X]$ et on identifie les coefficients de X^j dans chacun des deux membres). □

Remarque. d' est égal à la multiplicité de 0 dans P_k. On voit que l'étude des suites telles que $d' \geqslant 1$ se déduit sans peine de l'étude de celles pour lesquelles $d' = 0$.

Nous supposerons donc désormais que X ne divise pas $P_k(X)$, c'est-à-dire que l'entier q ne divise pas l'entier k.

Soit maintenant E l'ensemble des éléments de $\mathbb{F}_q[X]$ de degré strictement inférieur à $d^0 P_k$.

Considérons l'application ϱ de $\mathbb{N}$ vers E, qui à tout entier n associe le reste de la division de P_n par P_k. Pour tous entiers n et r tels que $r < q$, on remarque que $\varrho(nq + r)$ ne dépend que de $\varrho(n)$ et de $\varrho(r)$, qui ne prennent qu'un nombre fini de valeurs. On en déduit que l'idéal de A_q engendré par k est q-reconnaissable par $\mathscr{A} = (E, \{0, 1\}, 0, \varphi, \tau)$, où

$$\varphi : E \times \mathbb{N} \to E$$

$$(P, n) \to \varphi(P, n) = XP + \varrho(n) \text{ mod. } P_k,$$

et

$$\tau : E \to \{0, 1\}$$

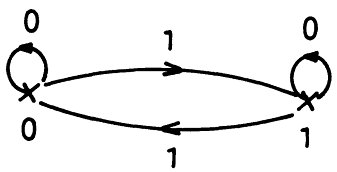
$$P \to \tau(P) = 0 \text{ si } P \neq 0$$

$$= 1 \text{ si } P = 0.$$

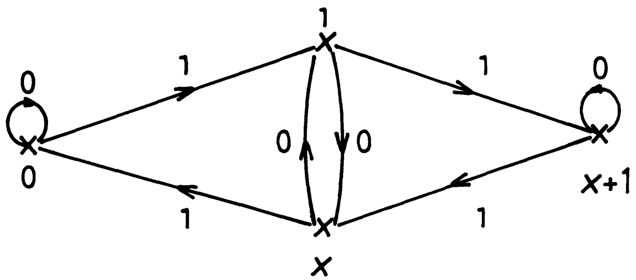
Théorème 1. *Tout idéal de A_q est q-reconnaissable.*

Exemples

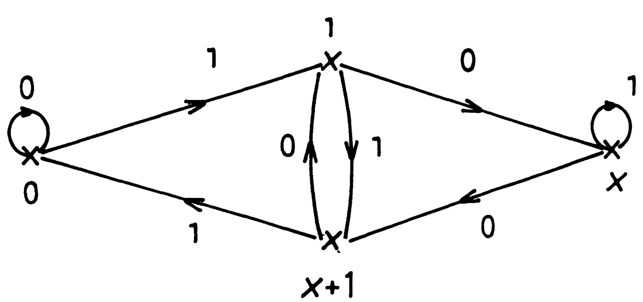
Exemple 1. L'idéal de A_2 engendré par 3 est formé des entiers $n = \Sigma_{r \geqslant 0}\, p_r(n) 2^r$ tels que $\Sigma_{r \geqslant 0}\, p_r(n)$ est pair (entiers de Morse); il est reconnu par le 2-automate:



EXEMPLE 2. L'idéal de A_2 engendré par 5 est formé des entiers $n = \Sigma_{r\geqslant 0}\, p_r(n)2^r$ tels que $\Sigma_{r\geqslant 0}\, p_{2r}(n)$ et $\Sigma_{r\geqslant 0}\, p_{2r+1}(n)$ sont pairs; il est reconnu par le 2-automate:

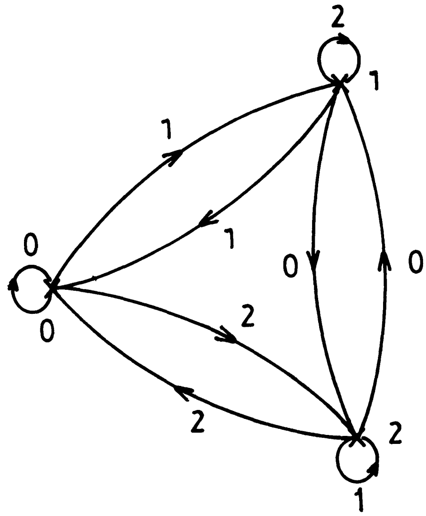


EXEMPLE 3. L'idéal de A_2 engendré par 7 est formé des entiers $n = \Sigma_{r\geqslant 0}\, p_r(n)2^r$ tels que $\Sigma_{r\geqslant 0}\, p_{3r}(n)$, $\Sigma_{r\geqslant 0}\, p_{3r+1}(n)$ et $\Sigma_{r\geqslant 0}\, p_{3r+2}(n)$ sont de même parité; il est reconnu par le 2-automate:



EXEMPLE 4. L'idéal de A_3 engendré par 4 est formé des entiers $n = \Sigma_{r\geqslant 0}\, p_r(n)3^r$ tels que $\Sigma_{r\geqslant 0}\, (-1)^r p_r(n)$ est un multiple de 3; il est reconnu

par le 3-automate:



2. Suite de nombres complexes associée à un idéal de A_q

L'application ϱ nous conduit à considérer une suite $u = (u_n)_{n\geqslant 0}$ à valeurs dans $\mathbb{U}$, qui nous permet d'associer injectivement à chaque élément de E un élément de $\mathbb{U}$. Il est ainsi naturel de poser pour tout entier n:

$$u_n = \prod_{r\geqslant 0} \mathrm{e}(p_r(\widetilde{\varrho(n)}(q)) \cdot q^{-(r+1)}).$$

Nous venons de voir que u est q-reconnaissable; on peut se demander à quelles conditions u est périodique ou q^h-multiplicative.

PROPOSITION 2. *Les 3 conditions suivantes sont équivalentes*
(*i*) *u est ultimement périodique.*
(*ii*) $k \in \{1, \ldots, q-1\}$
(*iii*) $\mathfrak{J}_q(k) = \mathbb{N}$.

DÉMONSTRATION. Tout élément de $\{1, \ldots, q-1\}$ étant inversible dans A_q, on a immédiatement ii $\Rightarrow$ iii $\Rightarrow$ i. Pour montrer que i $\Rightarrow$ ii, supposons qu'il existe $t \geqslant 1$ tel que $u_{n+t} = u_n$ à partir d'un certain rang. Pour h assez grand, on a

$$t < q^h \quad \text{et} \quad u_{q^h+t} = u_{q^h},$$

c'est-à-dire $P_t(X) = 0$ mod. $P_k(X)$. Posons $P_t(X) = t_0 + t_1X + \cdots + t_rX^r$, avec $t_r \neq 0$; pour h' assez grand, on a

$$u_{q^{h'}+(q-t_r)q^r} = u_{q^{h'}+(q-t_r)q^r+t}$$

et donc

$$(q - t_r)X^r = X^{r+1} + t_0 + t_1X + \cdots + t_{r-1}X^{r-1}$$

et

$$X^{r+1} = (q - t_r)X^r + t_rX^r = 0 \text{ mod. } P_k(X).$$

On en déduit, puisque l'on a supposé que X ne divisait pas $P_k(X)$, que $P_k(X)$ est un polynôme constant non nul, c'est-à-dire que $k \in \{1, \ldots, q - 1\}$. □

Remarque. Afin d'écarter ce cas banal, nous supposerons désormais que $k > q$, c'est-à-dire que P_k est un polynôme de degré d au moins égal à 1.

Proposition 3. *Il existe un entier non nul h tel que u soit q^h-multiplicative si et seulement si P_k est de degré égal à 1 (et dans ce cas u est q-multiplicative).*

Démonstration. Pour tous entiers n, a et b, avec $b < q^{hn}$ et $n \neq 0$, on a

$$u_{aq^{hn}+b} = \prod_{r<d} \mathrm{e}\left(\frac{p_r(\widetilde{\varrho(aq^{hn})}(q)) \oplus p_r(\widetilde{\varrho(b)}(q))}{q^{r+1}}\right)$$

$$= u_{aq^{hn}} \cdot u_b \cdot \prod_{r<d} \mathrm{e}\left(\frac{\varepsilon_r}{q^{r+1}}\right),$$

où

$$\varepsilon_r = -q \quad \text{si} \quad p_r(\widetilde{\varrho(aq^{hn})}(q)) + p_r(\widetilde{\varrho(b)}(q)) \geqslant q$$

$$= 0 \quad \text{sinon.}$$

Si $d = 1$,

$$\prod_{r<d} \mathrm{e}\left(\frac{\varepsilon_r}{q^{r+1}}\right) = 1$$

et u est q^h-multiplicative pour tout $h \geqslant 1$.

Si $d > 1$,

$$\prod_{r<d} \mathrm{e}\left(\frac{\varepsilon_r}{q^{r+1}}\right) = 1$$

pour tout (a, b, n) dans $\mathbb{N}^2 \times \mathbb{N}^*$ avec $b < q^{hn}$, si et seulement si $p_r(\widetilde{\varrho(aq^{hn})}(q)) + p_r(\widetilde{\varrho(b)}(q)) < q$ pour tout (a, b, n, r) dans $\mathbb{N}^2 \times \mathbb{N}^{*2}$ avec $b < q^{hn}$, ce qui implique $\varrho(aq^{hn}) = 0$ pour tout (a, n) dans $\mathbb{N} \times \mathbb{N}^*$. Or ceci est impossible puisque $P_k(X)$ ne divise pas X^{hn}. □

III. Etude spectrale q-adique de u

1. Etude de K_u^q

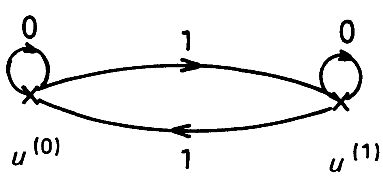
Puisque u_n ne dépend que de $\varrho(n)$ et que $\varrho(n \oplus n') = \varrho(n) + \varrho(n')$, on a le résultat remarquable suivant, qui nous conduit à entreprendre l'étude spectrale q-adique de la suite u:

PROPOSITION 4. *L'orbite de la suite u sous l'action du décalage q-adique est finie, de cardinal q^d.*

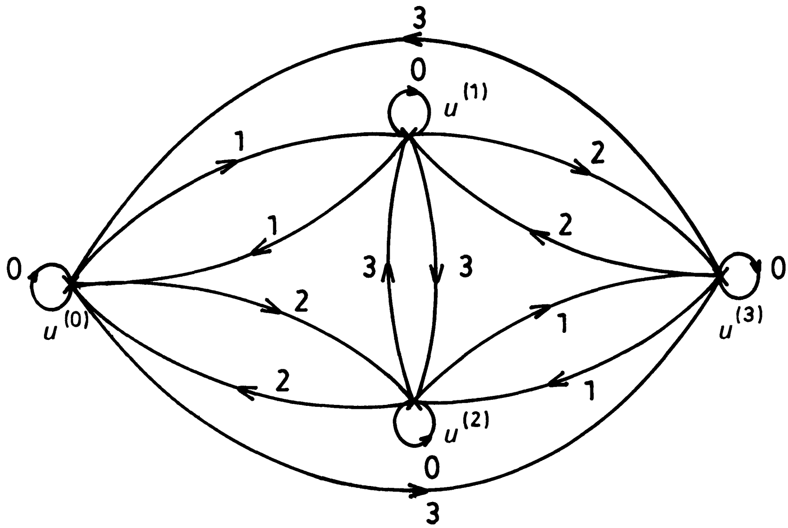
On peut décrire l'action du décalage q-adique sur u par un graphe de sommets $u^{(i)} = (u_{n\oplus i})_{n\in\mathbb{N}}$ pour $i < q^d$. Ce graphe, qui ne dépend que du degré du polynôme P_k, est isomorphe à celui de l'action du groupe $(\mathbb{F}_q[X]/(X^d), +)$.

Exemples

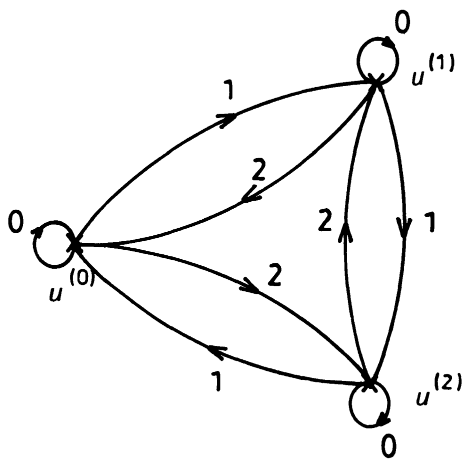
– L'action du décalage 2-adique sur la suite définie dans l'exemple 1 est décrite par le graphe:



– L'action du décalage 2-adique sur les suites définies dans les exemples 2 ou 3 est décrite par le graphe:



– L'action du décalage 3-adique sur la suite définie dans l'exemple 4 est décrite par le graphe:



COROLLAIRE. *Le G_q-flot associé à u est uniquement ergodique, l'unique mesure borélienne de probabilité sur K_u^q préservée par l'action du décalage q-adique étant la mesure d'équiprobabilité.*

2. Corrélations de u

Pour tout s dans $\mathbb{N}$ et pour tout $m = (m_0, \ldots, m_s)$ dans $\mathbb{Z}^{s+1}$, notons Π_m l'élément de $L^2(K_u^q, \mu_q)$ défini par:

$$\forall v \in K_u^q, \quad \Pi_m(v) = \Pi_{i \leqslant s} v_i^{m_i}.$$

L'ensemble $\{\Pi_m, m \in \mathbb{Z}^{s+1}\}$ engendre un sous-espace dense dans $L^2(K_u^q, \mu_q)$, et l'étude de l'ensemble des corrélations de Π_m lorsque m décrit $\mathbb{Z}^{s+1}$, appelées corrélations multiples de u, suffit à préciser le spectre de Walsh de u (cf. [11, 12]).

Pour tout entier N,

$$\frac{1}{N}\sum_{n<N} u_{n\oplus t}^{m_0} u_{n\oplus t\oplus 1}^{m_1} \ldots u_{n\oplus t\oplus s}^{m_s} \bar{u}_n^{m_0} \bar{u}_{n\oplus 1}^{m_1} \ldots \bar{u}_{n\oplus s}^{m_s}$$

$$= \frac{1}{N}\sum_{n<N} \mathrm{e}\left(\sum_{r<d}\sum_{i\leqslant s} m_i \frac{p_r(\tilde{\varrho}(n)(q)) + \varepsilon_{ir}}{q^{r+1}}\right)$$

où

$$\varepsilon_{ir} = -q \quad \text{si} \quad p_r(\tilde{\varrho}(t)(q)) + p_r(\tilde{\varrho}(n \oplus i)(q)) \geqslant q$$

$$= 0 \quad \text{sinon.}$$

On en déduit l'existence de $\gamma_{\Pi_m}^q$, que nous noterons γ_m:

$$\gamma_m(t) = \lim_{N\to+\infty} \frac{1}{N}\sum_{n<N} u_{n\oplus t}^{m_0} u_{n\oplus t\oplus 1}^{m_1} \ldots u_{n\oplus t\oplus s}^{m_s} \bar{u}_n^{m_0} \bar{u}_{n\oplus 1}^{m_1} \ldots \bar{u}_{n\oplus s}^{m_s}$$

$$= \frac{1}{q^d}\sum_{n<q^d} \mathrm{e}\left(\sum_{r<d}\sum_{i\leqslant s} m_i \frac{p_r(\tilde{\varrho}(n)(q)) + \varepsilon_{ir}}{q^{r+1}}\right)$$

qui ne dépend que de $\varrho(t)$. En particulier:

THÉORÈME 2. $(\gamma_m(t))_{t\in\mathbb{N}}$ *est q-reconnaissable, et il existe un polynôme B, de degré inférieur ou égal à* $(q^d - 1)$ *tel que* $\gamma_m(t) = B(u_t)$ *pour tout entier t.*

3. Spectre de Walsh de u

D'après le théorème 2, il suffit d'exhiber la mesure sur $\hat{G}_q$ dont la transformée de Fourier-Walsh est u pour en déduire le mesure associée à Π_m.

PROPOSITION 5. *La suite u est la transformée de Fourier–Walsh d'une combinaison linéaire finie à coefficients complexes de mesures de Dirac sur* $\hat{G}_q$.

DÉMONSTRATION. D'après la proposition 1, $\mathfrak{J}_q(k)$ est égal à l'ensemble des entiers naturels n vérifiant d étalités de la forme $\sigma_i(n) \equiv 0 \bmod. q$ $(i \in \{0, \ldots, d-1\})$ avec $\sigma_i(n) = \Sigma_{r \in \mathbb{N}} a_{ir} p_r(n)$ et $(a_{ir})_{r \in \mathbb{N}}$ une suite périodique d'entiers naturels.

Considérons l'application σ de G_q dans $\mathbb{F}_q^d$ qui, à tout entier n associe $(\sigma_i(n))_{i \in \{0, \ldots, d-1\}}$. σ et ϱ sont deux homomorphismes sujectifs de G_q dans $\mathbb{F}_q^d$ et E respectivement, qui ont pour noyau $\mathfrak{J}_q(k)$. Il s'en suit que les valeurs de σ et de ϱ sont en correspondance par un isomorphisme de groupes; plus précisément, il existe une matrice $B = (b_{ij})_{(i,j) \in \{0, \ldots, d-1\}^2}$ d'entiers naturels, telle que pour tout entier n,

$$(p_0(\varrho(n)(q)), \ldots, p_{d-1}(\varrho(n)(q))) = (\sigma_0(n), \ldots, \sigma_{d-1}(n))B \bmod. q.$$

On en déduit que pour tout entier n,

$$u_n = \prod_{j<d} \mathrm{e}(\sigma^{(j)}(n) \,.\, q^{-(j+1)})$$

où $\sigma^{(j)}(n)$ est l'élément de $\{0, \ldots, q-1\}$ tel que $\sigma^{(j)}(n) = \Sigma_{i<d} b_{ij} \sigma_i(n)$ mod. q.

Pour conclure, il nous suffit donc de donner, pour tout $j \in \{0, \ldots, d-1\}$, une mesure complexe μ à support fini sur $\hat{G}_q$ telle que $\mu = t$, avec $t(n) = \mathrm{e}(\sigma^{(j)}(n) \,.\, q^{-(j+1)})$. Pour cela, désignons par S_i l'élément $(\dot{a}_{i0}, \dot{a}_{i1}, \ldots)$ de $\hat{G}_q$, S la somme $\Sigma_{i<d} b_{ij} S_i$ et cherchons μ sous la forme $\mu = \Sigma_{k<d} c_k \delta_{kS}$ avec $(c_0, \ldots, c_{q-1}) \in \mathbb{C}^q$.

On a alors pour tout entier n:

$$\sum_{k<d} c_k \mathrm{e}\left(\frac{k\sigma^{(j)}(n)}{q}\right) = \mathrm{e}\left(\frac{\sigma^{(j)}(n)}{q^{j+1}}\right),$$

qui nous conduit, en considérant les différentes valeurs prises par $\sigma^{(j)}(n)$ à un système de Vandermonde admettant une unique solution $(c_0, \ldots, c_{q-1})$. $\square$

On en déduit:

THÉORÈME 3. *Le spectre de Walsh de u est discret, porté par le sous-groupe de* $\hat{G}_q$ *engendré par* $S_0, \ldots, S_{d-1}$.

IV. Etude spectrale classique de *u*

1. Rappels

Nous commençons par rappeler quelques résultats relatifs à l'étude spectrale des suites automatiques, contenus dans [14].

u étant q-reconnaissable, nous savons qu'elle est point fixe d'une substitution ζ de longueur constante égale à q, i.e., d'une application de $A = u(\mathbb{N})$ dans A^q, prolongée par concaténation à $A^{\mathbb{N}}$. On suppose que ζ est primitive, c'est à dire qu'il existe j tel que $\zeta^j(\alpha)$ contienne β pour tout $(\alpha, \beta) \in A^2$, et injective sur les lettres. On vérifie aisément que c'est le cas des substitutions associées aux suites que nous étudions. La suite

$$\left(\frac{1}{N} \sum_{n<N} \delta_{T^n u}\right)_{N \in \mathbb{N}}$$

n'a alors qu'une seule valeur d'adhérence.

On appelle valeurs propres de ζ les valeurs propres de l'opérateur U sur $L^2(K_u, \mu)$ défini par $Uf = f \circ T$. L'ensemble de ces nombres complexes est exactement l'ensemble des éléments de $\mathbb{U}$ chargés par le type spectral maximal σ_m de u. Une valeur propre de ζ est dite continue s'il existe une fonction continue de $L^2(K, \mu)$ qui lui soit associée.

La recherche des valeurs propres d'une substitution primitive conduit à introduire la notion suivante:

DÉFINITION 3. On appelle hauteur de ζ, et on note $h = h(\zeta)$, le nombre $\max\{n \geqslant 1;\ (n, q) = 1 \text{ et } n \mid pgcd\{j;\ u_j = u_o\}\}$.

On a alors:

THÉORÈME A [5]. *Les valeurs propres d'une substitution primitive non périodique ζ sont continues. Ce sont les nombres complexes de la forme* $\mathrm{e}(a)$, *où a décrit l'ensemble* $\mathbb{Z}(1/q) \times \mathbb{Z}/h\mathbb{Z}$, et $\mathbb{Z}(1/q)$ *note l'ensemble des rationnels q-adiques.*

On peut caractériser de plus le cas où ζ est de type spectral discret:

DÉFINITION 4. On dit que ζ, définie sue A de cardinal s, a une coïncidence s'il existe i et $j < q^i$ tels que $\zeta^i(0)_j = \zeta^i(1)_j = \cdots = \zeta^i(s-1)_j$.

THÉORÈME B [5]. *ζ est de type spectral discret si et seulement si ζ admet une coïncidence.*

Il reste dans le cas où ζ n'admet pas de coïncidence à préciser la composante continue de σ_m. On a pour cela un théorème particulièrement précis dans le cas où ζ est reconnue par un automate dont les instructions commutent entre elles et sont bijectives:

D étant le sous-groupe du tore engendré par $\{q^{-n}, n \in \mathbb{N}\}$, une mesure μ est dite D-quasi-invariante si $\mu * \delta_d \ll \mu$ pour tout $d \in D$.

THÉORÈME C [14 chap. IX]. *Si ζ est associée à un q'-automate bijectif et commutatif, le spectre de u est singulier; le type spectral maximal de u est équivalent à la somme des mesures D-quasi-invariantes obtenues à partir des produits de Riesz généralisés suivants:*

$$\prod_{n \in \mathbb{N}} \frac{|P_\chi(q'^n t)|^2}{q'},$$

où P_χ est le polynome trigonométrique

$$P_\chi(t) = \chi(\phi_0) + \chi(\phi_1)e^{it} + \cdots + \chi(\phi_{q'-1})e^{i(q'-1)t},$$

et où χ décrit le dual $\hat{G}$ du groupe G des instructions $\phi_0, \ldots, \phi_{q'-1}$ de l'automate, en supposant $\phi_0 = \mathrm{Id}$.

2. Valeurs propres de ζ

Les valeurs propres de ζ sont toutes continues, et leur étude se ramène à la détermination de la hauteur de ζ.

PROPOSITION 6. *ζ est une substitution de hauteur 1.*

DÉMONSTRATION. Quitte à remplacer k par $c \otimes k$ avec $c \in \{1, \ldots, q-1\}$, on peut supposer que la somme du premier et du dernier chiffre de k est supérieure ou égale à q. Donc k et $k \otimes (q^d + 1) = k(q^d + 1) - q^d$ sont premiers entre eux et $u_k = u_{k \otimes (q^d+1)} = 1$. □

On déduit du théorème A:

COROLLAIRE. *Le sous-groupe de $\mathbb{U}$ constitué des valeurs propres de ζ est égal au groupe des nombres complexes de la forme $\mathrm{e}(a)$ où a décrit l'ensemble $\mathbb{Z}(1/q)$ des rationnels q-adiques.*

q ne divisant pas k, ζ ne présente pas de coïncidence. D'après le théorème B, le type spectral maximal du système dynamique associé à ζ n'est donc pas discret; nous allons maintenant étudier sa composante continue.

3. Etude de la composante continue du type spectral maximal de u

Soit ℓ le plus petit entier naturel non nul tel que $X^{\ell} \equiv 1$ mod. P_k. Pour tout $(a, b) \in \mathbb{N}^2$, on a

$$u_{aq^{\ell}+b} = u_{\tilde{\varrho}(a)(q) \oplus \tilde{\varrho}(b)(q)}.$$

u est donc q^{ℓ}-reconnaissable par un automate dont les sommets et les flèches sont, aux étiquettes près, ceux du graphe décrit dans § III, 1. En particulier, ce q^{ℓ}-automate est bijectif et commutatif. Pour tout $j \in \{0, \ldots, q^{\ell} - 1\}$, notons ϕ_j la permutation sur $\mathbb{F}_q[X]/(P_k)$ qui à P associe $P + \varrho(j)$.

Soit G le groupe de permutations engendré par $\{\phi_j, j \in \{0, \ldots, q^d - 1\}\}$, qui est en fait le groupe de toutes les instructions du q^{ℓ}-automate; on remarque que G et $\hat{G}$ sont isomorphes à $(\mathbb{Z}/q\mathbb{Z})^d$. D'où le théorème suivant:

THÉORÈME 4. *Le spectre de u est simple et singulier. Le type spectral maximal σ_m est engendré par les produits de Riesz généralisés étrangers deux à deux*

$$\prod_{\substack{n \in \mathbb{N} \\ r < \ell}} \frac{\left| \sum_{j<q} \chi(\phi_{q^r})^j e^{ijq^{\ell n + r} t} \right|^2}{q^{\ell}}$$

où χ décrit $\hat{G}$.

En effet, les polynômes trigonométriques $P_\chi(t) = \Sigma_{j<q^{\ell}} \chi(\phi_j) e^{ijt}$ introduits au théorème C s'expriment, en écrivant l'indice j en base q, de la façon suivante:

$$P_\chi(t) = \prod_{r<\ell} \sum_{j<q} \chi(\phi_{q^r})^j e^{ijq^r t}.$$

Il nous reste à vérifier (cf. [14 chap. XI §2.]) que si $\chi \neq \chi'$ alors $|P_\chi| \neq |P_{\chi'}|$.

Posons pour tout $r \in \{0, \ldots, \ell - 1\}$ $\chi(\phi_{q^r}) = e(\varphi_r/q)$ avec $\varphi_r \in \{0, \ldots, q - 1\}$ (resp. $\chi'(\phi_{q^r}) = e(\varphi'_r/q)$ avec $\varphi'_r \in \{0, \ldots, q - 1\}$) et

$$Q_\chi(t) = \Pi_{r<\ell} (e^{i(q^r t + 2\pi\varphi_r/q)} - 1) \text{ (resp. } Q_{\chi'}(t) = \Pi_{r<\ell} (e^{i(q^r t + 2\pi\varphi'_r/q)} - 1)).$$

On a, pour tout $t \in \mathbb{R}\backslash(\pi.\ \mathbb{Z}(1/q))$

$$P_\chi(t) = \frac{\prod_{r<\ell} (e^{iq^r t} - 1)}{Q_\chi(t)}$$

et

$$P_{\chi'}(t) = \frac{\prod_{r<\ell} (e^{iq^r t} - 1)}{Q_{\chi'}(t)} .$$

Le théorème résulte donc du lemme suivant:

Lemme. *Si $\chi \neq \chi'$, il existe $t \in \mathbb{R}\backslash(\pi \cdot \mathbb{Z}(1/q))$ tel que $|Q_\chi(t)| \neq |Q_{\chi'}(t)|$.*

Démonstration. En effet si on avait $|Q_\chi(t)| = |Q_{\chi'}(t)|$ pour tout $t \in \mathbb{R}\backslash(\pi \cdot \mathbb{Z}(1/q))$, on aurait par continuité $|Q_\chi(t)| = |Q_{\chi'}(t)|$ pour tout réel t. D'où

$$\prod_{r<\ell} \left| \sin\left(q^r \frac{t}{2} + \frac{\varphi_r \pi}{q}\right)\right| = \prod_{r<\ell} \left| \sin\left(q^r \frac{t}{2} + \frac{\varphi'_r \pi}{q}\right)\right|$$

pour tout réel t, où l'on peut supposer $\varphi_{\ell-1} \neq \varphi'_{\ell-1}$ (quitte à simplifier les deux membres) et $\varphi_{\ell-1} \neq 0$ (quitte à échanger χ et χ'). Mais pour $t = -2\varphi_{\ell-1}\pi q^{-\ell}$, on aurait

$$\prod_{r<\ell} \left| \sin\left(q^r \frac{t}{2} + \frac{\varphi_r \pi}{q}\right)\right| = 0$$

et

$$\prod_{r<\ell} \left| \sin\left(q^r \frac{t}{2} + \frac{\varphi'_r \pi}{q}\right)\right| = \prod_{r<\ell} \left| \sin \frac{(q^{\ell-1}\varphi'_r - q^r \varphi_{\ell-1})\pi}{q^\ell}\right| > 0$$

ce qui conduirait à une contradiction. □

Exemples

– Dans le cas des entiers de la forme $3 \otimes_2 n$ (exemple 1), δ_0 et

$$\lambda = \prod_{n \in \mathbb{N}} \frac{|1 - e^{i2^n t}|^2}{2}$$

engendrent le type spectral maximal du système.

– Pour $5 \otimes_2 n$ (exemple 2), le type spectral maximal est engendré par

$$\delta_0, \lambda, \lambda_1 = \prod_{n \in \mathbb{N}} \frac{|1 + (-1)^n e^{i2^n t}|^2}{2}$$

et

$$\lambda_2 = \prod_{n \in \mathbb{N}} \frac{|1 - (-1)^n e^{i2^n t}|^2}{2}$$

– Pour $7 \otimes_2 n$ (exemple 3), le type spectral maximal est engendré par

$$\delta_0, \lambda_1' = \prod_{n \in \mathbb{N}} \frac{|1 + (-1)^{n+[n/3]+1} e^{i2^n t}|^2}{2},$$

$$\lambda_2' = \prod_{n \in \mathbb{N}} \frac{|1 + (-1)^{n+[(n+1/3)]} e^{i2^n t}|^2}{2},$$

et

$$\lambda_3' = \prod_{n \in \mathbb{N}} \frac{|1 + (-1)^{n+[(n+2/3)]} e^{i2^n t}|^2}{2}.$$

– Enfin, pour les entiers de la forme $4 \otimes_3 n$ (exemple 4), le type spectral maximal est engendré par

$$\delta_0, \lambda_1'' = \prod_{n \in \mathbb{N}} \frac{|1 + e((3 + (-1)^n)/6) e^{i.3^n t} + e((3 + (-1)^n)/3)\, e^{2i.3^n t}|^2}{3}$$

et

$$\lambda_2'' = \prod_{n \in \mathbb{N}} \frac{|1 + e((3 + (-1)^n)/3) e^{i.3^n t} + e((3 + (-1)^n)/6)\, e^{2i.3^n t}|^2}{3}.$$

On remarquera que l'analyse spectrale classique nous conduit à associer des objets assez compliqués à des suites qui sont définies par des propriétés arithmétiques très simples (sommes de chiffres en base q). Au contraire, l'analyse spectrale q-adique, bien adaptée à la description des propriétés des entiers écrits dans une base q, reflète cette simplicité.