ISRAEL JOURNAL OF MATHEMATICS, Vol. 64, No. 2, 1988

SUITES DE LONGUEUR MINIMALE ASSOCIEES A UN ENSEMBLE NORMAL DONNE

PAR

JEAN-PIERRE BOREL

Département de Mathématiques, U.F.R. des Sciences, 123, av. Albert Thomas, 87060 Limoges Cedex, France

ABSTRACT

For a given subset A of the set of real numbers, we search a sequence $\Lambda = (\lambda_n)$ of real numbers such that both A is the normal set $B(\Lambda)$ associated to Λ, and Λ takes its values in a bounded interval, with a minimal length M. A lower bound of M is obtained, which gives some necessary conditions of existency of such a bounded sequence Λ. More details are given when A is a subset of the set of integers. In this case, the problem is to find a polynomial Q of lowest degree such that the product $P.Q$ has non-negative coefficients, for some special given polynomial P.

1. Introduction: les ensembles normaux

1.1. Une suite $\Lambda = (\lambda_n)_{n \geqq 1}$ de nombres réels est dite équirepartie modulo 1 si on a:

$$(1) \qquad \forall x \in]0, 1], \qquad \lim_{N \to \infty} \frac{1}{N} \mathscr{A}(N, x, \Lambda) = x$$

où l'on pose

$$\mathscr{A}(N, x, \Lambda) = \sum_{n=1}^{N} \mathbf{1}_{[0,x[}(\{\lambda_n\}) = \operatorname{card}\{1 \leqq n \leqq N, \{\lambda_n\} < x\}.$$

1.2. Cette propriété peut s'interpréter comme la convergence étroite, dans l'ensemble $\mathscr{P}$ des probabilités sur $\mathbf{R}$, d'une suite de probabilités vers la

Reçu le 11 avril 1988

probabilité uniforme λ sur l'intervalle [0, 1]. En regardant les fonctions caractéristiques, définies pour $\mu \in \mathcal{P}$ par:

$$\varphi_\mu(t) = \int e^{itx} d\mu(x) = \hat{\mu}\left(-\frac{t}{2\pi}\right) \qquad (t \in \mathbf{R}),$$

et d'après un résultat dû à Paul Lévy (voir par exemple [REN], p. 299), (1) est alors équivalent à:

$$(2) \qquad \forall t \in \mathbf{R}, \qquad \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{it\{\lambda_n\}} = \varphi_\lambda(t) = \frac{e^{it}-1}{it}$$

(uniformément sur tout compact).

1.3. En fait, il suffit que (2) soit réalisé pour t décrivant $2\pi\mathbf{Z}$: une probabilité μ sur [0, 1] est déterminée par ses coefficients de Fourier $\hat{\mu}(k)$, $k \in \mathbf{Z}$. (1) est donc aussi équivalent à:

$$(3) \qquad \forall k \in \mathbf{N}^*, \qquad \lim_{N\to\infty} \frac{1}{N} \sum_{N=1}^{N} e^{2\pi i k \lambda_n} = 0.$$

C'est le critère de Weyl (voir [KUI]).

1.4. A la suite Λ, on peut associer un ensemble normal, partie de $\mathbf{R}$ définie par:

$$B(\Lambda) = \{x \in \mathbf{R},\ x\Lambda \text{ équirépartie modulo } 1\}$$

où $x\Lambda$ est la suite de terme général $x\lambda_n$. Cette notion a été introduite par M. Mendès-France, [MEN 1]. Une partie A de $\mathbf{R}$ est dite normale s'il existe une suite Λ telle que $A = B(\Lambda)$. Ces parties ont été caractérisées de façon simple par G. Rauzy dans [RAU].

THÉORÈME (Rauzy). *Une partie $A \subset \mathbf{R}$ est normale si et seulement si elle vérifie les trois propriétés suivantes*:

$$(4) \qquad \begin{cases} \text{(i) } 0 \notin A, \\ \text{(ii) } \forall k \in \mathbf{Z}^*,\ kA \subset A, \\ \text{(iii) } A \textit{ est élémentaire} \end{cases}$$

(une partie A de $\mathbf{R}$ est dite élémentaire lorsqu'il existe une suite f_n de fonctions continues telles que A est l'ensemble des x tels que $f_n(x)$ tend vers 0).

2. Le cas des suites bornées: présentation des résultats obtenus

2.1. Une partie A de $\mathbf{R}$ sera dite b-normale s'il existe une suite Λ bornée telle que $A = B(\Lambda)$. Deux problèmes se posent alors de façon naturelle:

(pb 1) caractériser les parties A de $\mathbf{R}$ qui sont b-normales;

(pb 2) pour une partie A b-normale, évaluer la borne minimale $M = M(A)$ associée:

$$M(A) = \inf\{M \geqq 0,\ \exists\,\Lambda, A = B(\Lambda) \text{ et } \forall\, n \geqq 1, 0 \leqq \lambda_n \leqq M\}.$$

Comme il est immédiat que $B(\Lambda) = B(\Lambda + c)$ pour toute constante c, on peut se restreindre à des suites à valeurs dans un intervalle $[0, M]$. Cela sera le cas dans toute la suite. Cette remarque justifie la définition de $M(A)$. Il est d'autre part clair que A b-normal revient à $M(A)$ fini.

2.2. Soit A une partie discrète de $\mathbf{R}$. On pose alors, pour $X > 0$:

$$\mathscr{A}(X) = \sum_{\substack{x \in A \\ |x| < X}} 1. \tag{5}$$

On appelle alors densité supérieure (resp. inférieure) de A la limite supérieure (resp. inférieure) de la quantité $(1/2X)\mathscr{A}(X)$, lorsque X tend vers l'infini. Elle est notée $\bar{d}(A)$ (resp. $\underline{d}(A)$).

On dira que A a une densité lorsque $\underline{d}(A) = \bar{d}(A)$, noté alors $d(A)$. De même, on posera:

$$s(A) = \sup_{X > 0} \frac{1}{2X}\, \mathscr{A}(X).$$

On a donc $0 \leqq \underline{d}(A) \leqq \bar{d}(A) \leqq s(a) \leqq +\infty$. Nous montrerons que toute partie A b-normale est discrète (résultat en fait déjà connu), et qu'il y a alors des liens entre $\underline{d}(A)$, $s(A)$ et $M(A)$.

THÉORÈME A. *Soit Λ une suite à valeurs dans $[0, M]$. L'ensemble normal $A = B(\Lambda)$ associé vérifie* (i), (ii), *et est discret dans* $\mathbf{R}$. *On a alors les majorations*:

$$\begin{cases} \text{(iv)} & \underline{d}(A) \leqq M, \\ \text{(v)} & s(A) \leqq 1.8M. \end{cases} \tag{6}$$

2.3. Une partie A de $\mathbf{R}$ vérifiant (i) et (ii), et discrète dans $\mathbf{R}$ peut s'écrire sous la forme:

$$(7)\qquad \begin{cases} A = \bigcup\limits_{k} \gamma_k \mathbf{Z}^*, \\ \forall k \geqq 0 \quad \gamma_{k+1} \notin A_k = \bigcup\limits_{i=1}^{k} \gamma_i \mathbf{Z}^*, \\ 0 < \gamma_1 < \gamma_2 < \cdots < \gamma_k < \cdots \end{cases}$$

où la suite des γ_k, soit finie soit infinie (et dans ce cas, γ_k croît vers $+\infty$ avec k), est uniquement déterminée par A (le cas $A = \varnothing$ sera ecarté dans toute la suite. Il est en effet clair que $\varnothing$ est b-normal, et que $M(\varnothing) = 0$: prendre $\lambda_n = 0$ pour tout entier n ...). On notera Γ la suite des γ_k et $A = \langle \Gamma \rangle$.

Il est alors facile de voir, par une méthode de convolution (par exemple, Mendès-France [MEN 2]), que si la série $\Sigma\, \gamma_k^{-1}$ converge (et c'est en particulier le cas lorsque les γ_k sont en nombre fini), alors A est b-normal, et l'on a:

$$M(A) \leqq \sum_k \gamma_k^{-1}.$$

La condition $\bar{d}(A) < +\infty$ n'entraine cependant pas que la série précédente converge. Nous montrerons que le théorème A entraine que l'hypothèse:

$$\exists\, C_0 \text{ absolue}, \qquad M(A) \leqq C_0 \bar{d}(A)$$

est fausse.

2.4. Dans le cas particulier $A \subset \mathbf{Z}$, la réponse au (pb 1) est connue. En effet, Dress et Mendès-France ont montré dans [DRE] qu'il existe Λ à valeurs dans $[0, 1]$ telle que $A = B(\Lambda)$, dès que A est une partie de $\mathbf{Z}$ vérifiant les conditions (i) et (ii). Par la même occasion, ils obtiennent la majoration $M(A) \leqq 1$.

Cela montre donc qu'il existe des ensembles b-normaux qui n'ont pas de densité: il existe des parties de $\mathbf{Z}$ vérifiant (i) et (ii) et n'ayant pas de densité asymptotique, cela a été montré par Besicovitch [BES]. Ces ensembles sont les "ensembles de multiples", voir [HAL, chap. V] pour de nombreux résultats les concernant.

2.5. Dans les paragraphes 4 à 6, nous étudierons la quantité $M(A)$ lorsque A est une partie b-normale de $\mathbf{Z}$. Une réponse est obtenue lorsque la suite des γ_k est finie, et dans ce cas une caractérisation des A tels que $M(A) = d(A)$ est donnée.

Théorème B. *Soit* $A = \bigcup_{i=1}^{k} \gamma_i \mathbf{Z}^*$ $(\gamma_i \in \mathbf{N}^*)$. *Alors* A *est b-normal,* $M(A) \geqq d(A)$, *et on a l'égalité si et seulement si le polynôme*:

$$P=\prod_{a\in\underline{A}}(X-\zeta_m^a)\qquad (m=\operatorname{ppcm}(\gamma_1,\gamma_2,\ldots,\gamma_k),\ \zeta_m=e^{2\pi i/m})$$

où $\underline{A}=A\cap\{1,2,\ldots,m-1\}$, *est à coefficients (entiers) positifs.*

Dans ce cas, une suite Λ *à valeurs dans* $[0,d(A)]$ *vérifie* $B(\Lambda)=A$ *si et seulement si* Λ *est* μ_0*-répartie, où* μ_0 *est la probabilité:*

$$\mu_0=\frac{1}{P(1)}\lambda_m * \mathop{*}_{a\in\underline{A}}(\delta_{1/m}-\zeta_m^a\delta_0).$$

2.6. Si $\mu\in\mathscr{P}$ est donné, on dit que Λ est μ-répartie (asymptotiquement) si les propriétés équivalentes (cf. 1.1 et 1.2) suivantes sont vérifiées:

$$\begin{cases}\forall x\in\mathbf{R},\quad \mu(\{x\})=0\Rightarrow \lim\limits_{N\to\infty}\dfrac{1}{N}\mathscr{A}(N,x,\Lambda)=\mu(]-\infty,x[),\\[2ex] \forall t\in\mathbf{R},\quad \lim\limits_{N\to\infty}\dfrac{1}{N}\sum\limits_{n=1}^{N}e^{it\lambda_n}=\varphi_\mu(t)=\hat{\mu}\left(-\dfrac{t}{2\pi}\right).\end{cases}$$

Si on note $\mathscr{Z}[\mu]$ l'ensemble des zéros de la transformée de Fourier $\hat{\mu}$, on a donc:

$$B(\Lambda)=\bigcap_{k=1}^{\infty}\left(\frac{1}{k}\mathscr{Z}[\mu]\right).\tag{8}$$

Etudier $B(\Lambda)$ revient donc à étudier les zéros de $\hat{\mu}$.

Une suite Λ (même bornée ...) n'a pas toujours une mesure de répartition asymptotique. Dans ce cas, on dira que $\mu\in\mathscr{P}$ est adhérente à Λ lorsqu'elle est adhérente (au sens de la convergence étroite) à la suite de probabilités:

$$\frac{1}{N}\sum_{n=1}^{N}\delta_{\lambda_n}.$$

De telles mesures existent toujours, et la relation (8) devient dans ce cas:

$$B(\Lambda)=\bigcap\left(\bigcap_{k=1}^{\infty}\left(\frac{1}{k}\mathscr{Z}[\mu]\right)\right),\tag{9}$$

où la première intersection porte sur l'ensemble des mesures μ adhérentes à la suite Λ (cette relation ne sera pas montrée ici).

3. Une condition nécessaire de b-normalité

3.1. Il est facile de voir que tout ensemble normal n'est pas nécessairement b-normal. Cela provient immédiatement du théorème A. La partie 3.2 de ce résultat est connue (Liardet, Rauzy, [LIA]), quoique l'auteur n'en connaisse pas de rédaction publiée. Cette démonstration est donc reprise pour des raisons de clarté de l'exposé.

Démonstration du théorème A

3.2. Considérons les fonctions holomorphes suivantes:

$$f_N(z)=\frac{1}{N}\sum_{n=1}^{N} e^{2\pi i\lambda_n z};\qquad g_N(z)=e^{-M\pi iz}f_N(z).$$

Soit $R>0$, fixé. On a alors, pour tout entier N:

$$|g_N(z)|\leqq \max_{1\leqq n\leqq N}|e^{2\pi i(\lambda_n-M/2)z}|\leqq e^{\pi M|\mathrm{Im}\, z|}.$$

On peut donc extraire une sous-suite $(g_{N_k})_{k\geqq 1}$ qui converge normalement, sur le disque $|z|\leqq R$, vers une fonction holomorphe g, qui vérifie donc en particulier:

$$g(0)=1\quad \text{et}\quad |g(Re^{i\theta})|\leqq e^{\pi RM|\sin\theta|}.$$

La fonction g n'est donc pas identiquement nulle, et le lemme de Jensen entraine:

$$\begin{aligned}\sum_{\substack{g(\rho)=0\\|\rho|<R}}\mathrm{Log}\frac{R}{|\rho|}&=\frac{1}{2\pi}\int_0^{2\pi}\mathrm{Log}|g(Re^{i\theta})|\,d\theta-\mathrm{Log}|g(0)|\\&\leqq\frac{RM\pi}{2\pi}\int_0^{2\pi}|\sin\theta|\,d\theta\\&=2RM\end{aligned}$$

(en remplaçant au besoin R par $R-\varepsilon$ si g a un zéro sur le cercle $|z|=R$).

Or, en utilisant (3) pour la suite $x\Lambda$ avec $k=1$, on obtient si $|x|<R$:

$$x\in B(\Lambda)\Rightarrow\lim_{N\to\infty}f_N(x)=0\Rightarrow\lim_{N\to\infty}g_N(x)=0\Rightarrow g(x)=0.$$

D'où la majoration:

$$\sum_{\substack{x \in A \\ |x| < R}} \operatorname{Log} \frac{R}{|x|} \leqq 2RM \qquad (\text{pour tout } R > 0). \tag{10}$$

On déduit immédiatement de cette inégalité que A est discret dans $\mathbf{R}$, et que $s(A) \leqq eM$:

$$\frac{1}{2R} \sum_{\substack{x \in A \\ |x| < R}} 1 \leqq \frac{1}{2R} \sum_{\substack{x \in A \\ |x| < eR}} \operatorname{Log} \frac{eR}{|x|} \leqq \frac{2eRM}{2R} = e\,.\,M.$$

3.3. La majoration de $\underline{d}(A)$ s'obtient par une sommation à la Abel. Posons:

$$\mathscr{S}(R) = \sum_{\substack{x \in A \\ \gamma \leqq x \leqq R}} \operatorname{Log} \frac{R}{x}$$

où γ est le plus petit élément strictement positif de A (si $A = \varnothing$, $d(A) = 0 \leqq M$). On a alors, d'après (10):

$$RM \geqq \mathscr{S}(R) = \sum_{\substack{x \in A \\ \gamma \leqq x \leqq R}} \int_x^R \frac{dt}{t} = \int_\gamma^R \frac{\mathscr{A}(t)}{t}\, dt$$

$$\geqq \underline{d}(A)R + o(R) + O(1)$$

cela entraine donc (iv).

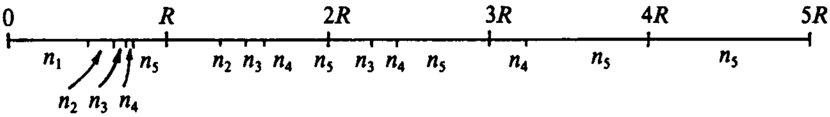
3.4. On a évidemment $\bar{d}(A) \leqq s(A) \leqq eM$. Cependant, l'ensemble A vérifie la propriété (ii), ce qui lui donne une certaine "régularité" qui permet d'améliorer cette majoration. En effet, elle entraîne:

$$\forall R > 0, \quad \forall i \in \mathbf{N}, \qquad \mathscr{A}((i+1)R) - \mathscr{A}(iR) \geqq \mathscr{A}(R) - \mathscr{A}\left(\frac{i}{i+1} R\right). \tag{11}$$

Soit R positif quelconque, et posons:

$$\begin{cases} 2n_1 = \mathscr{A}(\tfrac{1}{2}R), \\ 2n_i = \mathscr{A}\left(\dfrac{i}{i+1} R\right) - \mathscr{A}\left(\dfrac{i-1}{i} R\right), \quad 2 \leqq i \leqq 4, \\ 2n_5 = \mathscr{A}(R) - \mathscr{A}(\tfrac{4}{5}R). \end{cases}$$

Le nombre d'éléments de la suite A dans chacun des intervalles ci-dessous peut alors être minoré comme indiqué, en utilisant la minoration (10):



La majoration (10), appliquée au point 5.R, donne donc:

$$\begin{aligned} 2R\,.\,M \geqq\; & (\mathrm{Log}\ 10)n_1 + (\mathrm{Log}\ \tfrac{15}{2} + \mathrm{Log}\ \tfrac{15}{4})n_2 + (\mathrm{Log}\ \tfrac{20}{3} + \mathrm{Log}\ \tfrac{10}{3} + \log \tfrac{20}{9})n_3 \\ & + (\mathrm{Log}\ \tfrac{25}{4} + \mathrm{Log}\ \tfrac{25}{8} + \mathrm{Log}\ \tfrac{25}{12} + \mathrm{Log}\ \tfrac{25}{16})n_4 \\ & + (\mathrm{Log}\ 5 + \mathrm{Log}\ \tfrac{5}{2} + \mathrm{Log}\ \tfrac{5}{3} + \mathrm{Log}\ \tfrac{5}{4})n_5 \\ \geqq\; & (\mathrm{Log}\ 10)(n_1 + n_2 + n_3 + n_4 + n_5) + (\mathrm{Log}\ \tfrac{125}{48})(n_2 + n_3 + n_4 + n_5). \end{aligned}$$

Soit $\varepsilon > 0$ fixé, et R fixé tel que $\mathscr{A}(R) \geqq (s(A) - \varepsilon)\,.\,2R$. Pour une telle valeur de R, on a:

$$n_1 + n_2 + n_3 + n_4 + n_5 = \tfrac{1}{2}\mathscr{A}(R) \geqq (s(A) - \varepsilon)\,.\,R,$$

$$n_2 + n_3 + n_4 + n_5 = \tfrac{1}{2}(\mathscr{A}(R) - \mathscr{A}(R/2)) \geqq (\tfrac{1}{2}s(A) - \varepsilon)\,.\,R,$$

ce qui donne, en faisant tendre ε vers 0:

$$5M \geqq (\mathrm{Log}\ 10)s(A) + (\tfrac{1}{2}\,\mathrm{Log}\ \tfrac{125}{48})s(A)$$

d'où

$$s(A) \leqq \frac{5}{\mathrm{Log}\ 10 + \frac{1}{2}\,\mathrm{Log}\ \frac{125}{48}}\,M = 1{,}79782\ldots M.$$

3.5. Erdös a montré dans [ERD] que, si on prend $\gamma_i = k + i$, avec $1 \leqq i \leqq k$, l'ensemble A_k associé vérifie:

$$\lim_{k \to \infty} d(A_k) = 0.$$

Corollaire. *Il n'existe pas de constante absolue C telle que, pour tout ensemble A b-normal, on ait $M(A) \leqq C\bar{d}(A)$.*

Démonstration. D'après [DRE], les ensembles A_k définis ci-dessus sont b-normaux, et il est clair que l'on a:

$$\forall k \geqq 1 \qquad s(A_k) \geqq \tfrac{1}{2} \qquad \text{(ou même Log 2).}$$

On obtient donc, pour tout k, et en utilisant (v):

$$\frac{M(A_k)}{\bar{d}(A_k)} = \frac{M(A_k)}{d(A_k)} \geqq \frac{1}{3.6\ d(A_k)}$$

qui tend vers $+\infty$ avec k.

On peut même trouver des ensembles A_k qui vérifient simultanément:

$$\text{(12)} \qquad \begin{cases} \lim_{k \to \infty} d(A_k) = 0, \\ \\ \lim_{k \to \infty} s(A_k) = 1. \end{cases}$$

En effet, si on pose $\Gamma_k = \{k, k+1, \ldots, [k^{3/2}]\}$ et $A_k^{(1)} = \langle \Gamma_k \rangle$, on a:

$$\lim_{k \to \infty} d(A_k^{(1)}) = 0 \qquad \text{d'après [TEN], théorème 1,}$$

$$\lim_{k \to \infty} s(A_k^{(1)}) = 1 \qquad \text{car } s(A_k^{(1)}) \geqq k^{-3/2}([k^{3/2}] - k).$$

On peut aussi remarquer que $s(A) = 1$ entraine trivialement $\bar{d}(A) = 1$.

3.6. Le cas particulier $A = \mathbf{Z}^*$ montre de façon immédiate que la majoration (iv) est optimale.

4. Une méthode de régularisation

4.1. Soit $\mu \in \mathscr{P}$, et x un nombre réel positif. On notera alors:

$$\begin{cases} \mu'[x] = \sum_{n \in \mathbf{Z}} \mu([nx, (n+1)x[)\delta_{nx}, \\ \\ \mu[x] = \mu'[x] * \lambda_x, \end{cases}$$

où λ_x désigne la probabilité uniforme sur l'intervalle $[0, x]$.

$\mu'[x]$ et $\mu[x]$ sont donc deux probabilités sur $\mathbf{R}$, la première discrète, la seconde absolument continue. D'autre part, si X est une variable aléatoire réelle de loi μ, $\mu'[x]$ est la loi de la variable

$$Y = x\left[\frac{1}{x} X\right].$$

4.2.

Théorème C. *Soient b et m deux entiers positifs, m multiple de b. Soit Λ une suite de nombres réels et $\mu \in \mathscr{P}$ une probabilité adhérente à Λ. Alors $b\mathbf{Z}^* \subset B(\Lambda)$ entraine $b\mathbf{Z}^* \subset \mathscr{Q}[\mu[1/m]]$.*

Démonstration. Les hypothèses μ adhérente à Λ et $b\mathbf{Z}^* \subset B(\Lambda)$ entrainent $b\mathbf{Z}^* \subset \mathscr{Q}[\mu]$. Posons:

$$B = \{b, 2b, \ldots, m-b\} = \{k.b, 1 \leqq k \leqq m/b - 1\}.$$

Comme $\mathscr{Q}[\lambda_{1/m}] = m\mathbf{Z}^*$, il suffit donc de montrer que l'on a l'inclusion $B + m\mathbf{Z} \subset \mathscr{Q}[\mu'[1/m]]$, et comme $\mu'[1/m]$ est périodique de période m, $B \subset \mathscr{Q}[\mu'[1/m]]$ suffit.

Soit X une variable aléatoire réelle de loi μ, et

$$Y = \frac{1}{m}[mX].$$

Alors Y est de loi $\mu'[1/m]$. Posons $m = ab$. Alors

$$bY = \frac{1}{a}[ab\,X].$$

L'hypothèse $b\mathbf{Z}^* \subset \mathscr{Q}[\mu]$ entraine que bX est uniforme modulo 1, et donc:

$$Z = (b.Y \bmod 1) \quad \text{est équirépartie sur} \quad \left\{0, \frac{1}{a}, \ldots, \frac{a-1}{a}\right\}.$$

Si ν est la loi de $b.Y$, cette propriété se traduit par $\{1, 2, \ldots, a-1\} \subset \mathscr{Q}[\nu]$, et donc par $B \subset \mathscr{Q}[\mu'[1/m]]$.

4.3. Supposons $A = \langle \gamma_1, \gamma_2, \ldots, \gamma_k \rangle$ avec des γ_i entiers positifs. En appliquant k fois le théorème, avec m et $b = \gamma_i$ (notation du 2.3), on obtient alors immédiatement:

Corollaire 1. *Si $A \subset B(\Lambda)$, avec $A = \bigcup_{i=1}^{k} \gamma_i \mathbf{Z}^*$ ($\gamma_i \in \mathbf{N}^*$), et si μ est adhérente à Λ, on a:*

$$A \subset \mathscr{Q}\left[\mu\left[\frac{1}{m}\right]\right] \qquad \text{où } m = \operatorname{ppcm}(\gamma_1, \gamma_2, \ldots, \gamma_k).$$

On peut en déduire que $A \subset B(\Lambda')$ si Λ' est une suite $\mu[1/m]$-répartie. Cela n'augmente que modérement l'intervalle où varient les λ_n, puisque si Λ est à valeurs dans $[0, M]$, on peut prendre Λ' à valeurs dans $[0, M']$ avec $M' = M + 1/m$.

4.4. Supposons Λ à valeurs dans $[0, M]$, et μ adhérente à Λ. Alors en notant $\lceil x \rceil$ le plus petit entier supérieur x, on a pour $m \geqq 1$:

$$\mu'[1/m] = \sum_{n=0}^{\lceil mM \rceil - 1} \rho_n \delta_{n/m}$$

et donc si on pose $X = e^{2\pi i t/m}$:

$$\widehat{\mu'[1/m]}(-t) = \sum_{n=0}^{\lceil nM \rceil - 1} \rho_n X^n = Q(X). \tag{13}$$

COROLLAIRE 2. *Soit* $A = \bigcup_{i=1}^{k} \gamma_i \mathbf{Z}^*$ $(\gamma_i \in \mathbf{N}^*)$, $m = \mathrm{ppcm}(\gamma_1, \gamma_2, \ldots, \gamma_k)$, *et P le polynôme*:

$$P = \prod_{a \in \underline{A}} (X - \zeta_m^a),$$

où $\underline{A} = A \cap \{1, 2, \ldots, m-1\}$.

Soit Λ *une suite à valeurs dans* $[0, M]$ *telle que* $A \subset B(\Lambda)$, *et* μ *adhérente à* Λ. *Alors P divise le polynôme Q défini par* (13).

En particulier, on a:

$$M \geqq d(A).$$

DÉMONSTRATION. Si $a \in \underline{A}$, $t = a$ n'annule pas $\hat{\lambda}_{1/m}$. Il annule donc, d'après le corollaire 1, $\widehat{\mu'[1/m]}$. Cela signifie que ζ_m^a est racine de Q. Q est donc divisible par P. Cela entraine en particulier:

$$\lceil mM \rceil - 1 = d^0 Q \geqq d^0 P = \mathrm{card}\, \underline{A} = md(A) - 1$$

et donc $mM \geqq md(A) - 1$ (car $md(A)$ est entier).

Cela entraine donc $M \geqq d(A) - 1/m$. Or, dans le théorème, on peut remplacer m par un multiple $c.m$, $c \geqq 1$. Il en est donc de même ici, et donc $M \geqq d(A)$.

On retrouve donc le résultat (iv) obtenu au chapitre 3, dans ce cas particulier.

4.5. Le théorème B se déduit aussi du théorème C et de ses deux corollaires:

DÉMONSTRATION DU THÉORÈME B. A est b-normal d'après [DRE], et $M(A) \geqq d(A)$ provient du corollaire 2.

Si $M(A) = d(A)$, on peut appliquer le corollaire 2 à toute probabilité μ

adhérente à une suite Λ à valeurs dans $[0, d(A)]$. On a alors $d^0P = d^0Q$, et donc:

$$Q = \frac{1}{P(1)} P$$

puisque $Q(1) = \|\mu\| = 1$. Q étant à coefficients positifs, il en est de même pour P. Réciproquement, si P est à coefficients positifs, la mesure μ_0 associée vérifie $\mathcal{Q}[\mu_0] = A$, et a pour support l'intervalle $[0, d(A)]$.

Supposons maintenant Λ suite à valeurs dans $[0, d(A)]$, m' multiple de m, et μ adhérente à Λ. Le corollaire 2 entraine donc si on pose $m' = mm''$:

$$\begin{cases} \widehat{\mu'\left[\dfrac{1}{m'}\right]}(-t) = Q'(X') \\ \quad \text{avec } X' = e^{2\pi i t/m'}, \quad Q \text{ polynôme de degré } m'd(A) - 1; \\ Q' \text{ divisible par} \\ \quad P' = \displaystyle\prod_{\substack{a \in A \\ 1 \leq a \leq m'-1}} (X' - \zeta_{m'}^a) = P(X'^{m''}) . (1 + X' + X'^2 + \cdots + X'^{m''+1}), \end{cases}$$

qui provient de la relation $A \cap \{1, 2, \ldots, m' - 1\} = \underline{A} . \{1, 2, \ldots, m''\} \cup \{1, 2, \ldots, m'' - 1\} . m'$. On a donc $d^0P' = m''d^0P + m'' - 1 = m'd(A) - 1$. On obtient donc:

$$Q' = \frac{1}{P'(1)} P'$$

et en particulier les coefficients de Q' sont constants sur toute tranche de la forme $\{cm'', cm'' + 1, \ldots, cm'' + m'' - 1\}$. Cela n'est possible que si μ a une densité uniforme sur tout intervalle de la forme $[c/m, (c + 1)/m]$, puisque le résultat précédent est vrai pour tout m''. On obtient donc nécessairement:

$$\mu = \mu[1/m] = \mu_0$$

(condition suffisante d'après ce qui précède).

5. Le cas P à coefficients positifs

5.1. Le polynôme P du théorème B est de la forme:

$$P = \prod_{j \in J} \frac{(X^{r_j} - 1)}{(X^{s_j} - 1)} .$$

Des critères ont été obtenus pour que ce type d'expression ait des coefficients positifs, lorsqu'elle représente un polynôme: voir par exemple Grosswald [GRO], Reich [REI]. Mais ces critères sont très loin d'être utilisables. Pour m entier, on pose:

$$\phi_m(X) = \frac{X^m - 1}{X - 1} = 1 + X + X^2 + \cdots + X^{m-1}.$$

5.2.

PROPOSITION. *Soient* $\gamma_1 < \gamma_2 < \cdots < \gamma_k < \gamma_{k+1}$ *des nombres entiers et posons*:

$$\begin{cases} m = \mathrm{ppcm}(\gamma_1, \gamma_2, \dots, \gamma_k), \quad m' = \mathrm{ppcm}(m, \gamma_{k+1}) = m, m''' = \gamma_{k+1} m'', \\ A = \bigcup_{i=1}^{k} \gamma_i \mathbf{Z}^*, \quad \underline{A} = A \cap \{1, 2, \dots, m-1\}, \\ A' = A \cup \gamma_{k+1}\mathbf{Z}^*, \quad \underline{A}' = A' \cap \{1, 2, \dots, m'-1\}, \\ P = \prod_{a \in \underline{A}} (X - \zeta_m^a), \quad P' = \prod_{a' \in \underline{A}'} (X - \zeta_{m'}^{a'}). \end{cases}$$

On a alors:

$$P'(X) = P(X^{m'''}) \phi_{m'''}(X) \frac{\phi_{m''}(X)}{\prod_{a'' \in \underline{A}''} (X - \zeta_{m''}^{a''})} \tag{14}$$

avec $A'' = \bigcup_{i=1}^{k} \gamma_i'' \mathbf{Z}^*$, *où* $\gamma_i'' = \gamma_i / (\gamma_{k+1}, \gamma_i)$ $(1 \leqq i \leqq k)$, *et* $\underline{A}'' = A'' \cap \{1, 2, \dots, m''-1\}$.

DÉMONSTRATION. On a, pour $1 \leqq i \leqq k$:

$$\gamma_i \mid n \quad \text{et} \quad \gamma_{k+1} \mid n \Leftrightarrow \gamma_i'' \gamma_{k+1} \mid n$$

et donc:

$$A' = A \cup \gamma_{k+1}(\mathbf{Z}^* - A'')$$

où la réunion est disjointe. D'où la relation:

$$\begin{aligned} \underline{A}' = (\underline{A} + m \,.\, \{0, 1, \dots, m''' - 1\}) \cup (m \,.\, \{1, 2, \dots, m''' - 1\}) \\ \cup (\gamma_{k+1} \,.\, (\{1, 2, \dots, m'' - 1\} - \underline{A}'')) \end{aligned} \tag{15}$$

ce qui donne exactement la formule cherchée, puisque l'on a:

$$\prod_{a' \in \underline{A} + m.\{0,2,\ldots,m'''-1\}} (X - \zeta_{m'}^{a'}) = \prod_{a \in \underline{A}} \prod_{i=0}^{m'''-1} (X - \zeta_{m'}^{a} \zeta_{m'''}^{i}) = \prod_{a \in \underline{A}} (X^{m''} - \zeta_m^a) = P(X^m),$$

$$\prod_{a' \in m.\{1,2,\ldots,m'''-1\}} (X - \zeta_{m'}^{a'}) = \sum_{i=0}^{m'''-1} (X - \zeta_{m'''}^{i}) = \phi_{m'''}(X),$$

$$\prod_{a' \in \gamma_{k+1}(\{1,2,\ldots,m''-1\} - \underline{A}'')} (X - \zeta_{m'}^{a}) = \frac{\phi_{m''}(X)}{\prod_{a' \in \gamma_{k+1}\underline{A}''} (X - \zeta_{m'}^{a'})} = \frac{\phi_{m''}(X)}{\prod_{a'' \in \underline{A}''} (X - \zeta_{m''}^{a''})} .$$

5.3. La proposition précédente permet de calculer P pour les petites valeurs de k:

$k = 1$: $m = \gamma_1$ $P = 1$ (a tous ses coefficients strictement positifs).

$k = 2$: on peut supposer $(\gamma_1, \gamma_2) = d$, $\gamma_i = d\gamma_i'$, d'où $m = d\gamma_1'\gamma_2'$.

On obtient alors:

$$P = \phi_{\gamma_1'}\phi_{\gamma_2'} \quad \text{(a tous ses coefficients strictement positifs).}$$

$k = 3$: on peut supposer $(\gamma_1, \gamma_2, \gamma_3) = 1$ (cela ne change pas P), et on pose:

$$\gamma_1 = \gamma_2'\gamma_3'\beta_1, \quad \gamma_2 = \gamma_3'\gamma_1'\beta_2, \quad \gamma_3 = \gamma_1'\gamma_2'\beta_3,$$

avec $1 = (\beta_1, \beta_2) = (\beta_2, \beta_3) = (\beta_3, \beta_1)$. On obtient alors $m = \gamma_1'\gamma_2'\gamma_3'\beta_1\beta_2\beta_3$ et:

$$P = \phi_{\gamma_2'\beta_1}(X^{\beta_3})\phi_{\gamma_1'\beta_2}(X^{\beta_3})\phi_{\beta_3}\frac{\phi_{\gamma_3'\beta_1\beta_2}}{\phi_{\beta_1}\phi_{\beta_2}}$$

$$= \phi_{\gamma_2'\beta_1}(X^{\beta_3})\frac{\phi_{\gamma_1'\beta_2\beta_3}}{\phi_{\beta_2}}\frac{\phi_{\gamma_3'\beta_2\beta_3}}{\phi_{\beta_1}}$$

et en remarquant que l'on a $\phi_{ab}/\phi_b = \phi_a(X^b)$, on obtient:

$$P = \phi_{\gamma_2'\beta_1}(X^{\beta_3})\phi_{\gamma_1'\beta_3}(X^{\beta_2})\phi_{\gamma_3'\beta_2}(X^{\beta_1}) \qquad \text{(a tous ses coefficients positifs)}$$

mais P peut avoir des coefficients nuls: si par exemple $\beta_i \geqq 2$ $(1 \leqq i \leqq 3)$, le coefficient de X dans P est nul.

$k = 4$: la formule devient très compliquée dans le cas général. Elle se simplifie si on suppose $\gamma_1, \gamma_2, \gamma_3, \gamma_4$ premiers entre eux deux à deux. La proposition donne alors:

$$P = \phi_{\gamma_1}(X^{\gamma_3\gamma_4})\phi_{\gamma_3}(X^{\gamma_2\gamma_4})\phi_{\gamma_2}(X^{\gamma_1\gamma_4})\phi_{\gamma_4}\frac{\phi_{\gamma_1\gamma_2\gamma_3}}{\phi_{\gamma_1}(X^{\gamma_3})\phi_{\gamma_3}(X^{\gamma_2})\phi_{\gamma_2}(X^{\gamma_1})} ,$$

$$P = \phi_{\gamma_1}(X^{\gamma_3\gamma_4})\phi_{\gamma_3}(X^{\gamma_2\gamma_4})\phi_{\gamma_2}(X^{\gamma_1\gamma_4})\phi_{\gamma_4}\,\frac{\phi_{\gamma_1}(X^{\gamma_2\gamma_3})}{\phi_{\gamma_1}(X^{\gamma_3})\phi_{\gamma_2}(X^{\gamma_1})}\,.$$

La fraction est un polynôme, mais on n'a plus de renseignement sur le signe de ses coefficients, et donc de même pour P. Ils ne sont pas toujours positifs ou nuls, puisque le calcul montre que:

si $\gamma_1 = 2$, $\gamma_2 = 3$, $\gamma_3 = 5$, $\gamma_4 = 7$:

$$P = 1 + 2X + 2X^2 + X^3 \quad - X^5 - X^6 - X^7 - X^8 - X^9$$

$$+ X^{11} + 2X^{12} + 2X^{13} + 2X^{14} + \cdots + X^{161}$$

(voir en 6.6 le tableau de tous les coefficients de P dans ce cas). Si par contre on prend $\gamma_1 = 6$, $\gamma_2 = 10$, $\gamma_3 = 14$, $\gamma_4 = 15$ (qui ne sont pas premiers entre eux ...), alors le polynôme P associé est à coefficients positifs.

$k = 5$: La formule générale devient beaucoup trop longue à écrire. Si l'on prend $\gamma_1 = 2$, $\gamma_2 = 3$, $\gamma_3 = 5$, $\gamma_4 = 7$, $\gamma_5 = 11$, le polynôme P associé est de degré 1829, et ses coefficients prennent exactement toutes les valeurs entières comprises entre -7 et 9.

6. Le cas où P a des coefficients négatifs

6.1. Soit P un polynôme à coefficients réels. Si P a une racine dans $\mathbf{R}_+^*$, il ne peut avoir tous ses coefficients positifs ou nuls, et de même pour tout produit PQ.

LEMMA. *Soit $z = \rho e^{i\theta}$, avec $-\pi < \theta \leqq \pi$ et $\theta \neq 0$. Le polynôme:*

$$P_{n,z} = P_n = X^{2^{n+1}} - 2\cos(2^n\theta)\rho^{2^n}X^{2^n} + \rho^{2^{n+1}}$$

admet z pour racine, et est à coefficients positifs si

$$n = n_z = \left[\frac{\operatorname{Log}(\pi/|\theta|)}{\operatorname{Log} 2}\right].$$

DÉMONSTRATION. La seconde propriété est immédiate, puisque l'on a alors $\pi/2 < 2^n|\theta| \leqq \pi$.

D'autre part:

$$\begin{aligned}P_n(z) &= \rho^{2^{n+1}}(e^{i2^{n+1}\theta} - 2\cos(2^n\theta)e^{i2^n\theta} + 1)\\ &= \rho^{2^{n+1}}\left(e^{i2^{n+1}\theta} - 2\,\frac{e^{i2^n\theta}+e^{-i2^n\theta}}{2}\,e^{i2^n\theta} + 1\right)\\ &= 0.\end{aligned}$$

Donc si P n'a pas de racines dans $\mathbf{R}_+^*$, il existe un polynôme Q tel que PQ ait tous ses coefficients strictement positifs, par exemple:

$$PQ = \prod_{P(z)=0} P_{n_z,z}.$$

Dans ce qui suit, on notera:

$\delta = \delta(P) = \min(d^0Q)$, minimum pris sur tous les polynômes Q tels que PQ ait tous ses coefficients positifs ou nuls;

$\delta^+ = \delta^+(P) = \min(d^0Q)$, minimum pris sur tous les polynômes Q tels que:

soit (P1): PQ a tous ses coefficients strictement positifs,

soit (P2): PQ a tous ses coefficients positifs ou nuls, et Q n'a pas de racine de module 1.

EXEMPLE. $P = X^2 - X + 1 = (X - e^{i\pi/3})(X - e^{-i\pi/3})$.

Alors $(X+1)P = X^3 + 1$. Donc $\delta(P) = 1$.

$(aX+b)P$ ne peut avoir tous ses coefficients positifs ou nuls que si $a = b$. Donc $\delta^+(P) \geqq 2$. Or on a:

$$(2X^2 + 4X + 3)P = 2X^4 + 2X^3 + X^2 + X + 3$$

et donc $\delta^+(P) = 2$.

6.2. En fait, dans la définition de $\delta^+(P)$, (P2) suffit: si en effet Q vérifie (P1), le polynôme $Q(\lambda X)$ vérifie aussi (P1) pour λ assez voisin de 1. On peut alors choisir un tel λ tel que $Q(\lambda X)$ n'a pas de racine de module 1, ce qui donne un polynôme de même degré que Q et vérifiant (P2).

C'est la propriéte (P2) qui sera en fait utilisée plus tard, mais la propriété (P1) permet des évaluations plus rapides de $\delta^+(P)$. Par exemple, si Q est tel que PQ ait tous ses coefficients positifs ou nuls, et si r est le nombre maximal de coefficients consécutifs nuls dans PQ, on obtient:

$$PQ\phi_{r+1} \quad \text{a tous ses coefficients strictement positifs}$$

et donc

$$\delta^+(P) \leqq \delta(P) + r.$$

En fait, ce n'est pas tout à fait (P2) qui est utile, mais une propriété plus compliquée, qui est conséquence de (P2). Cette propriété ne peut s'écrire que pour les polynômes P du type considéré, c'est-à-dire

$$P = \prod_{a \in A} (X - \zeta_m^a).$$

Elle s'écrit alors:

(P2'): PQ a ses coefficients positifs ou nuls, et toute racine ρ de Q de module 1 vérifie:

$$\exists \kappa \geqq 2, \quad \rho^\kappa \neq 1 \quad \text{et } P(\rho^\kappa) \neq 0 \quad \text{et} \quad Q(\rho^\kappa) \neq 0.$$

Enfin, on peut remarquer que si P est un polynôme réciproque (i.e. $P = P^* := X^{d^0P} P(1/X)$), les polynômes Q de degré minimaux satisfaisant (P1) ou (P2) ou même (P2') peuvent être eux aussi choisis réciproques (sinon, on remplace Q par $Q + Q^*$...).

6.3. On note comme précédemment $A = \bigcup_{i=1}^k \gamma_i \mathbf{Z}^*$, $\gamma_1 < \gamma_2 < \cdots < \gamma_k$ entiers, $m = \text{ppcm}(\gamma_1, \gamma_2, \ldots, \gamma_k)$, et:

$$P = \prod_{a \in A} (X - \zeta_m^a).$$

Théorème D. *A est b-normal, et on a lorsque P a au moins un coefficient négatif:*

$$d(A) + \frac{\delta(P)}{m} \leqq M(A) \leqq d(A) + \frac{\delta^+(P)}{m} \leqq 1.$$

Démonstration. A b-normal est déjà connu (et se retrouve ici, puisque l'on va montrer $M(A) \leqq 1$).

Soit Λ à valeur dans $[0, M]$ telle que $A = B(\Lambda)$. Alors d'après le corollaire 2 du théorème C, on a lorsque μ est adhérente à Λ et Q défini par (13):

P divise Q,

Q a ses coefficients positifs ou nuls,

$d^0Q = \lceil mM \rceil - 1 \leqq mM.$

En considérant le polynôme R tel que $Q = PR$, on obtient:

$$\delta(P) \leqq d^0R = d^0Q - d^0P \leqq mM + md(A) - 1.$$

D'où la minoration $d(A) + (\delta(P) - 1)/m \leqq M(A)$.

6.4. En fait, la minoration précédente est encore valable si on remplace m par un multiple $m' = mm''$, P étant alors remplacé par P' défini par:

$$P'(X) = P(X^{m''})\phi_{m''}(X).$$

LEMME. *Soit $k \geqq 1$ et P donnés, et soit P' le polynôme $P(X^k)\phi_k(X)$. On a alors*

$$\delta(P') = k\delta(P) \quad et \quad \delta^+(P') \leqq k\delta^+(P).$$

DÉMONSTRATION. Soit Q tel que PQ ait tous ses coefficients dans $\mathbf{R}_+$, et soit Q' le polynôme $Q'(X) = Q(X^k)$. Alors $P'Q'$ a tous ses coefficients dans $\mathbf{R}_+$. Donc $\delta(P') \leqq k\delta(P)$.

De même: si PQ a tous ses coefficients dans $\mathbf{R}_+^*$, il en est de même pour $P'Q'$; si Q n'a pas de racine de module 1, Q' aussi.

Donc $\delta^+(P') \leqq k\delta^+(P)$.

Soit maintenant Q' tel que $P'Q'$ ait tous ses coefficients positifs. On pose:

$$Q'(X) = \sum_{j=0}^{d} c'_j X^j, \qquad Q(X) = \sum_{j=0}^{[d/k]} c_j X^j \qquad \text{avec } c_j = \sum_{f=kj}^{kj+k-1} c'_f,$$

$$P(X) = \sum_{j=0}^{h} e_j X^j, \qquad \text{d'où } P'(X) = \sum_{j=0}^{kh+k-1} e_{[j/k]} X^j,$$

et cela entraine l'identité, pour tout entier j:

$$\sum_{h+i=j} e_i c_h = \sum_{h+i=jk+k-1} e_{[i/k]} c'_h .$$

Le polynôme PQ a donc tous ses coefficients positifs ou nul. Donc en prenant Q' de degré $\delta(P')$:

$$\delta(P) \leqq \left[\frac{\delta(P')}{k}\right] \leqq \frac{\delta(P')}{k} .$$

Cela termine la démonstration du lemme.

On obtient donc, en revenant à la démonstration du théorème:

$$\forall\, m'' \geqq 1 \qquad M(A) \geqq d(A) + \frac{\delta(P') - 1}{m'} = d(A) + \frac{\delta(P)}{m} - \frac{1}{mm''}$$

ce qui donne la minoration annoncée.

6.5. Soit maintenant Q de degré minimal, correspondant à la définition de $\delta^+(P)$, et tel que Q n'a pas de racine de module 1. On pose:

$$Q(X)=\sum_{j=0}^{\delta^+(P)} c_j X^j,$$

$$\mu=\left(\sum_{j=0}^{\delta^+(P)} c_j\delta_{j/m}\right)*\left(\mathop{*}_{a\in A}(\delta_{1/m}-\zeta_m^a\delta_0)\right)*\lambda_{1/m}.$$

Comme Q n'a pas de racine sur le cercle unité,

$$\hat{\mu}(-t)=Q(e^{2\pi it/m})P(e^{2\pi it/m})\times\frac{e^{2\pi it/m}-1}{2\pi it/m}$$

admet A pour ensemble de ses zéros.

Si Q satisfait (P2′), on a encore

$$A=\bigcap_{j=1}^{\infty}\left(\frac{1}{k}\mathscr{Q}[\mu]\right).$$

Si on choisit Λ μ-répartie, à valeurs dans le support de μ (contenu dans $[0,(1+d^0PQ)/m]$), on obtient $B(\Lambda)=A$. Donc:

$$M(A)\leqq\frac{1+d^0P+d^0Q}{m}=d(A)+\frac{\delta^+(P)}{m}.$$

Il reste à remarquer que P divise ϕ_m, dont les coefficients ont strictement positifs, et donc:

$$\delta^+(P)\leqq m-1-d^0P=m(1-d(A)).$$

6.6. Nous allons ici présenter un exemple d'évaluation exacte de la quantité $M(A)$, dans un cas régi par le théorème D.

Dans l'exemple du 4.3, avec $k=4$, on obtient facilement $\delta(P)\leqq\alpha_1\alpha_3+\alpha_1\alpha_2-2$. Pour $\alpha_1=2$, $\alpha_2=3$, $\alpha_3=5$, $\alpha_4=7$, on a donc $\delta(P)\leqq 14$. En utilisant l'expression de P dans ce cas, on vérifie que:

$$\delta(P)=6,\qquad \delta^+(P)=6.$$

En effet, P est de degré 161 et ses coefficients sont donnés dans le tableau suivant:

1	2	2	1	0	−1	−1	−1	−1	−1	0	1	2	2	2	2	2	1	0	−1	−1	0	1	1	1	1	1	1	1	1
1	1	1	1	1	2	3	3	2	1	0	0	0	0	0	1	2	3	3	3	3	3	2	1	0	0	1	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	1	0	0	1	2	3	3	3	3	3	2	1	0	0	0
0	0	1	2	3	3	2	1	1	1	1	1	1	1	1	1	1	1	1	1	0	−1	−1	0	1	2	2	2	2	2
1	0	−1	−1	−1	−1	−1	0	1	2	2	1																		

Comme P est réciproque, on cherche simplement parmi les polynômes Q réciproques, d'après 6.2. Or on a:

$\cdot\,\delta(P) \leqq 4$ est impossible: $PQ(1) > 0$ entraine $Q(1) > 0$, et si $d^0 Q \leqq 4$, le coefficient de X^n, avec $n = 5 + d^0 Q$, dans PQ, vaut $-Q(1)$.

$\cdot\,\delta(P) = 5$ est impossible: si $Q = a + bX + cX^2 + cX^3 + bX^4 + aX^5$, et si PQ a ses coefficients positifs ou nuls, on a:

$$\begin{cases} a > 0 & \text{coefficient de } X^0 \text{ dans } PQ, \\ 2b + 4c \geqq 0 & \text{coefficient de } X^4, \\ -b - 2c \geqq 0 & \text{coefficient de } X^8, \\ 2b + 3c \geqq 0 & \text{coefficient de } X^5, \\ -a - 2b - 2c \geqq 0 & \text{coefficient de } X^9. \end{cases}$$

On peut donc choisir $a = 1$, et nécessairement $b = -2c$. Alors on doit avoir $c \leqq 0$ et $c \geqq \frac{1}{2}$.

• Si $Q_0 = 5 - 4X - X^2 + 6X^3 - X^4 - 4X^5 + 5X^6$, le polynôme $P.Q_0$ a tous ses coefficients positifs ou nuls, donnés par le tableau:

5	6	1	1	5	0	0	1	0	0	4	0	0	1	5	6	6	2	6	6	5	6	6	1	5	5	0	1	6	6
6	6	6	6	6	11	12	7	7	11	6	6	7	6	6	10	6	6	7	11	11	12	8	12	12	11	12	12	7	11
11	6	7	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	12
12	12	12	12	12	12	12	12	12	12	12	12	12	12	12	7	6	11	11	7	12	12	11	12	12	8	12	11	11	7
6	6	10	6	6	7	6	6	11	7	7	12	11	6	6	6	6	6	6	6	1	0	5	5	1	6	6	5	6	6
2	6	6	5	1	0	0	4	0	0	1	0	0	5	1	1	6	5												

On peut remarquer que si Q est de degré 6 (et $Q = Q^*$) et si PQ a ses coefficients positifs, alors ses coefficients de X^6 et X^9 sont nuls (car opposés l'un de l'autre). Il n'existe donc pas de polynôme Q de degré $\leqq 6$ tel que PQ ait tous ses coefficients strictement positifs.

D'autre part, si on pose $Y = X + X^{-1}$, on a:

$$Q_0 = X^3(5Y^3 - 4Y^2 - 16Y + 14)$$

ce qui permet de vérifier que Q_0 a six racines de module 1, dont les arguments θ vérifient:

$$-2\cos\theta \in \{-1{,}81433\ldots;\ 0{,}900452\ldots;\ 1{,}713879\ldots\}$$

et donc Q_0 n'a pas de racine de la forme $e^{2\pi i n/240}$, $n \in \mathbf{N}$. Donc Q_0 satisfait (P2′), et $\delta^+(P) = 6$.

Comme $\delta = \delta^+$ ici, on en déduit:

$$M(2\mathbf{Z}^* \cup 3\mathbf{Z}^* \cup 5\mathbf{Z}^* \cup 7\mathbf{Z}^*) = \frac{168}{210} = \frac{4}{5}\,.$$

QUATRE REMARQUES.

On peut voir ici que $s(A_0) = \frac{9}{10} = \frac{9}{8}M(A_0)$.

Il n'y a pas unicité de la distribution des suites Λ à valeurs dans $[0, M(A_0)]$ telles que $A_0 = B(\Lambda)$: le polynôme $Q = 6 - 5X - X^2 + 7X^3 - X^4 - 5X^5 + 6X^6$ marche aussi, ce qui donne une infinité de mesures $\mu \in \mathscr{P}$ possibles, à support dans $[0, \frac{4}{5}]$, telles que:

$$A_0 = \bigcap_{k=1}^{\infty} \frac{1}{k}\,\mathscr{Q}[\mu].$$

Cela permet par exemple de construire des suites Λ à valeurs dans $[0, \frac{4}{5}]$, telles que $A_0 = B(\Lambda)$, et n'ayant pas de mesure de répartition asymptotique. Ce phénomène n'est pas général: si on prend $A_1 = 2\mathbf{Z}^* \cup 3\mathbf{Z}^* \cup 5\mathbf{Z}^* \cup 11\mathbf{Z}^*$, le polynôme P associé est de degré 129 et a ses coefficients variant entre -1 et 3. Dans ce cas, $\delta(P) = \delta^+(P) = 3$, et il y a unicité (à une constante multiplicative près) de Q de degré 3, et donc de la répartition des suites associées à A_1 et de longueur minimale.

La méthode de convolution conduit pour A_0 à un polynôme de degré 243 (c'est à dire à une suite Λ dans l'intervalle $[0, 122/105]$, ce qui est bien moins bon), dont les coefficients sont positifs mais très grands (ils varient entre 1 et 86091).

Il est possible de montrer que, si A est b-normal et si A' est une partie de A vérifiant la condition (ii), alors A' est b-normal et vérifie $M(A') \leqq 2M(A)$ (voir [BOR]). Donc, en revenant à l'écriture de A donnée en (7), on en déduit que si l'on pose:

$$A_n = \bigcup_{k \leqq n} \gamma_k \mathbf{Z}^*$$

alors A est b-normal si et seulement si la suite des $M(A_n)$ est bornée, et plus précisément:

$$\tfrac{1}{2}\sup M(A_n) \leqq M(A) \leqq 2\ \underline{\lim}\ M(A_n).$$

Cela justifie donc l'intérêt du calcul de la quantité $M(A)$ lorsque l'ensemble Γ associé est fini: une formule "explicite" en fonction des γ_k permettrait alors de caractériser les ensembles b-normaux. Il va de soi qu'un tel calcul explicite paraît très difficile ... .

Bibliographie

[BES] A. S. Besicovitch, *On the density of certain sequences of integers*, Math. Ann. **110** (1934), 336–341.

[BOR] J.-P. Borel, *Parties d'ensembles b-normaux*, Manuscr. Math. **62** (1988), 317–335.

[DRE] F. Dress et M. Mendès-France, *Caractérisation des ensembles normaux dans* **Z**, Acta Arith. **17** (1970), 115–120.

[ERD] P. Erdös, *Note on sequences of integers no one of which is divisible by any other*, J. London Math. Soc. **10** (1935), 126–128.

[GRO] E. Grosswald, *Reducible rational fractions of the type of Gaussian polynomials with only non negative coefficients*, Bull. Can. Math. **21** (1978), 21–30.

[HAL] H. Halberstam and K. F. Roth, *Sequences*, Vol. I, Clarendon Press, Oxford, 1966.

[KUI] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, Wiley–Interscience, New York, 1974.

[LIA] P. Liardet et G. Rauzy, Communication personnelle.

[MEN 1] M. Mendès-France, *Deux remarques concernant l'équirépartition des suites*, Acta Arith. **14** (1968), 163–167.

[MEN 2] M. Mendès-France, *La réunion des ensembles normaux*, J. Number Theory **2** (1970), 354–351.

[RAU] G. Rauzy, *Caractérisation des ensembles normaux*, Bull. Soc. Math. France **98** (1970), 401–414.

[REI] D. Reich, *On certain polynomials of Gaussian type*, Can. J. Math. **31** (1979), 274–281.

[REN] A. Rényi, *Calcul des probabilités*, Dunod, Paris, 1966.

[TEN] G. Tenenbaum, *Sur la probabilité qu'un entier possède un diviseur dans un intervalle donné*. Compos. Math. **51** (1984), 243–263.