Relations de récurrence linéaires, primitivé et loi de Benford

Autor(en): **Deligny, Hugues / Jolissaint, Paul**

Objekttyp: **Article**

Zeitschrift: **Elemente der Mathematik**

Band (Jahr): **68 (2013)**

PDF erstellt am: **25.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-515890

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

Elem. Math. 68 (2013) 9 – 21
0013-6018/13/010009-13
DOI 10.4171/EM/213

© Swiss Mathematical Society, 2013

Elemente der Mathematik

Relations de récurrence linéaires, primitivité et loi de Benford

Hugues Deligny et Paul Jolissaint

Hugues Deligny est professeur agrégé de mathématiques au collège Titan, Le Port, La Réunion. Ses centres d'intérêt sont les mathématiques pour l'informatique, en particulier les notions de complexité, d'entropie, de profondeur logique, automates cellulaires, et hasard effectif.

Paul Jolissaint est professeur associé à temps partiel à l'Université de Neuchâtel et professeur de physique et de mathématiques au Lycée cantonal de Porrentruy. Son domaine de recherche se situe en algèbres d'opérateurs et en théorie ergodique.

1 Introduction

Nous nous intéressons ici à la loi de Benford pour des suites $(a_n)_{n\geq 1} \subset \mathbb{R}^+$ qui satisfont une relation de récurrence d'ordre k de la forme :

$$a_{n+k} = c_{k-1}a_{n+k-1} + c_{k-2}a_{n+k-2} + \ldots + c_1 a_{n+1} + c_0 a_n \qquad (\star)$$

avec les conditions initiales $a_i > 0$ pour tout $1 \leq i \leq k$. On supposera la plupart du temps que les coefficients c_i sont positifs ou nuls, et que $c_0 > 0$, de sorte que la relation

Das Benfordsche Gesetz lässt sich in vielen realen Datensätzen beobachten. Es besagt, dass die Anfangsziffer $d \in \{1, \ldots, 9\}$ mit der Häufigkeit $\log_{10}(1 + 1/d)$ auftritt. Die Anfangsziffer 1 kommt mit über 30% also deutlich häufiger vor, als die 9 mit weniger als 5%. Für Zufallszahlen einer gegebenen Wahrscheinlichkeitsverteilung lässt sich rechnerisch nachprüfen, ob sie dem Benfordschen Gesetz gehorchen. Auch bei Zahlenfolgen kann man die Frage nach der Gültigkeit des Benforschen Gesetzes stellen. Genau das tun die Autoren der vorliegenden Arbeit für Folgen, die einer linearen Rekursion $a_{n+k} = c_{k-1}a_{n+k-1} + c_{k-2}a_{n+k-2} + \ldots + c_1 a_{n+1} + c_0 a_n$ genügen. Paul Jolissaint hat in früheren Arbeiten hinreichende Bedingungen für die Gültigkeit des Benfordschen Gesetzes aus den Nullstellen des charakteristischen Polynoms abgeleitet. Hier werden nun die Bedingungen direkt an den Koeffizienten $c_0, \ldots, c_{k-1}$ festgemacht.

de récurrence soit effectivement d'ordre k. On va présenter des conditions suffisantes sur les c_i pour qu'il existe (au moins) un entier $b > 2$ tel que la suite $(a_n)_{n\geq 1}$ satisfasse la loi de Benford en base b.

Rappelons qu'étant donné un tel entier $b > 2$, une suite $(u_n)_{n\geq 1} \subset \mathbb{R}^+ \setminus \{0\}$ satisfait la *loi de Benford en base* b si, pour tout $t \in [1, b)$, on a :

$$\lim_{N\to\infty} \frac{|\{1 \leq n \leq N \ : \ M_b(u_n) < t\}|}{N} = \log_b(t),$$

où $M_b(u_n)$ désigne la *mantisse* de u_n, c'est-à-dire l'unique élément de $[1, b)$ tel que $u_n = M_b(u_n) \cdot b^m$ avec $m \in \mathbb{Z}$ (cf. [5, définition 2.1]). La définition ci-dessus généralise le cas classique qui correspond à $b = 10$ (dix) et qui affirme que le premier chiffre significatif $d_1(u_n)$ de u_n satisfait la loi de probabilité (cf. remarque (2) de [5]) :

pour tout chiffre $1 \leq d \leq 9$, on a

$$\lim_{N\to\infty} \frac{|\{1 \leq n \leq N : d_1(u_n) = d\}|}{N} = \log_{10}\Big(1 + \frac{1}{d}\Big).$$

D'après les théorèmes principaux de [4] et [5], une suite $(u_n) \subset \mathbb{R}^+ \setminus \{0\}$ satisfait la loi de Benford en base b dès qu'elle remplit les deux conditions suivantes :

(a) il existe des nombres réels $\alpha > 0$, $\rho > 0$ et μ tels que $\lim_{n\to\infty} \frac{u_n}{n^\mu \rho^n} = \alpha$;

(b) $\log_b(\rho)$ est irrationnel.

Si c'est le cas, si $Q(x)$ est un polynôme non constant à coefficients entiers et $Q(x) \geq 1$ pour x assez grand, la sous-suite $(u_{Q(n)})_{n\geq 1}$ satisfait également la loi de Benford en base b.

L'exemple suivant découle immédiatement des deux conditions ci-dessus, et il ne semble pas avoir été découvert auparavant :

Exemple 1. Soit $(p_n)_{n\geq 1}$ la suite croissante des nombres premiers. Comme cela a été observé dans [3], la suite (p_n) ne satisfait pas la loi de Benford. En revanche, choisissons deux entiers $\ell \geq 2$ et $b > 2$ tels que $\log_b(\ell)$ soit irrationnel. Alors la suite (p_{ℓ^n}) satisfait la loi de Benford en base b. En effet, par le théorème des nombres premiers, on a

$$\lim_{n\to\infty} \frac{p_n}{n \ln(n)} = 1.$$

En passant à la sous-suite $(\ell^n)_{n\geq 1} \subset \mathbb{N}^*$, on a

$$\lim_{n\to\infty} \frac{p_{\ell^n}}{n\ell^n \ln(\ell)} = 1 \quad \text{et donc} \quad \lim_{n\to\infty} \frac{p_{\ell^n}}{n\ell^n} = \ln(\ell).$$

Dans le cas d'une suite $(a_n)_{n\geq 1}$ qui satisfait une relation de récurrence du type $(\star)$, $(a_n)_{n\geq 1}$ s'exprime à l'aide des racines du *polynôme caractéristique* de la relation de récurrence, c'est-à-dire le polynôme

$$p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0.$$

Plus précisément, écrivons $p(x) = (x - \zeta_1)^{\mu_1} \cdots (x - \zeta_m)^{\mu_m}$ oú $\zeta_1, \ldots, \zeta_m \in \mathbb{C}$ sont les zéros distincts de $p(x)$ de multiplicités respectives $\mu_1, \ldots, \mu_m \geq 1$. Alors $(a_n)_{n\geq 1}$ est une

combinaison linéaire des k suites $(n^\ell \zeta_j^n)_{n\geq 1}$ pour $0 \leq \ell < \mu_j$ et $1 \leq j \leq m$: il existe des constantes $\alpha_{j,\ell}$ dépendant des conditions initiales $a_1, \ldots, a_k$ telles que

$$a_n = \sum_{j=1}^{m} \sum_{\ell=0}^{\mu_j - 1} \alpha_{j,\ell} n^\ell \zeta_j^n \quad \forall n \geq 1.$$

Dès lors, si $p(x)$ admet une racine positive simple ρ telle que $|\zeta| < \rho$ pour toute autre racine ζ de $p(x)$ et si le coefficient de ρ^n est positif dans la décomposition ci-dessus, alors la suite $(a_n)_{n\geq 1}$ satisfait la condition (a).

Il nous a semblé intéressant de donner des conditions suffisantes sur les *coefficients* de la relation de récurrence ($\star$) plutôt que sur les *racines* du polynôme caractéristique de la relation de récurrence. Nous mettrons plus particuliérement l'accent sur le cas où les coefficients c_i sont positifs ou nuls.

Le premier résultat de notre étude est :

Théorème 2. *Soient $c_0, c_1, \ldots, c_{k-1}$ des nombres réels. On pose*

$$I = \{1 \leq j \leq k-1 : c_j \neq 0\},$$

et on suppose que $I \neq \emptyset$. Enfin, on associe à la suite $c_0, \ldots, c_{k-1}$ le polynôme

$$p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0.$$

(1) *Si les c_i sont positifs ou nuls et si $c_0 > 0$, le polynôme p admet une unique racine positive ρ et $|\zeta| < \rho$ pour tout autre zéro ζ de p (compté avec multiplicité) si, et seulement si* $\mathrm{pgcd}(I \cup \{k\}) = 1$.

(2) *Si $c_{k-1} \geq 2$ et si $c_{k-1} > \sum_{j=0}^{k-2} |c_j| + 1$, alors le polynôme p admet une racine simple $\rho \in]c_{k-1} - 1, c_{k-1} + 1[$, et toute autre racine ζ de p satisfait $|\zeta| < 1$.*

(3) *Soit $b > 2$ un entier tel que $\log_b(\rho)$ soit irrationnel, et soit une suite $(a_n)_{n\geq 1} \subset \mathbb{R}^+ \setminus \{0\}$ qui satisfait la relation de récurrence*

$$a_{n+k} = c_{k-1}a_{n+k-1} + \ldots + c_1 a_{n+1} + c_0 a_n.$$

Si les c_i satisfont la condition (1) *ou la condition* (2)*, et dans ce dernier cas si de plus a_n ne tend pas vers 0 lorsque $n \to \infty$, alors la suite $(a_n)_{n\geq 1}$ satisfait la loi de Benford en base b. Enfin, il en est de même de toute sous-suite de la forme $(a_{Q(n)})$ où $Q(x)$ désigne un polynôme non constant à coefficients entiers tel que $Q(x) \geq 1$ pour tout x suffisamment grand.*

Remarque. La condition supplémentaire $a_n \not\to 0$ dans la troisième affirmation du théorème ci-dessus est indispensable. En effet, la suite $a_n = 10^{-n}$ tend vers 0, satisfait la relation de récurrence

$$a_{n+2} = \frac{31}{10}a_{n+1} - \frac{3}{10}a_n$$

dont le polynôme caractéristique est $p(x) = (x-3)(x-1/10)$; ses coefficients satisfont la condition (2) du théorème, mais la suite ne satisfait pas la loi de Benford pour $b = 10$, bien que $\log_{10}(3)$ soit irrationnel.

On verra que lorsque les c_i sont positifs ou nuls, le polynôme caractéristique $p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0$ admet toujours une racine dominante $\rho > 0$, c'est-à-dire telle que $|\zeta| \leq \rho$ pour toute autre racine ζ ; regardons maintenant le cas où il admet $h > 1$ racines $\zeta_1 = \rho, \ldots, \zeta_h$ telles que $|\zeta_j| = \rho$. On note encore $I = \{1 \leq j < k : c_j > 0\}$, et pour tout $m \in \{0, \ldots, h-1\}$, on pose

$$I_m = \{j \in I : j \equiv m \pmod h\}$$

de sorte que $(I_m)_{0 \leq m < h}$ constitue une partition de I.

Théorème 3. *Soient $c_0 > 0, c_1 \geq 0, \ldots, c_{k-1} \geq 0$, et h comme ci-dessus. Alors $h = \mathrm{pgcd}(I \cup \{k\})$. De plus, toute suite $(a_n)_{n\geq 1}$ qui satisfait la relation de récurrence*

$$a_{n+k} = c_{k-1}a_{n+k-1} + c_{k-2}a_{n+k-2} + \ldots + c_1 a_{n+1} + c_0 a_n$$

avec des conditions initiales positives ou nulles $a_1, \ldots, a_k$ est réunion des h sous-suites $(a_{m+hn})_{n\geq 1}$, $0 \leq m < h$. Enfin, pour tout $0 \leq m < h$, on a l'alternative suivante :
- *Si $\{j \in I_m : a_j > 0\} \neq \emptyset$, alors $\lim_{n\to\infty} \frac{a_{m+hn}}{\rho^n}$ existe et est positive, et la suite $(a_{m+hn})_{n\geq 1}$ satisfait la loi de Benford en base b pour tout b tel que $\log_b(\rho) \notin \mathbb{Q}$.*
- *Si $\{j \in I_m : a_j > 0\} = \emptyset$, alors $a_{m+hn} = 0$ pour tout $n \geq 1$.*

Exemple 4. Le théorème 2 s'applique au cas des *suites de Fibonacci d'ordre $k \geq 2$* : on choisit des nombres réels $a_1, \ldots, a_k > 0$ arbitraires, et on définit $(a_n)_{n\geq 1}$ par

$$a_{n+k} = a_{n+k-1} + a_{n+k-2} + \ldots + a_{n+1} + a_n.$$

Notons que la racine dominante $\rho > 0$ est irrationnelle grâce à l'observation suivante :

Proposition 5. *Soit $k \geq 2$ un entier et soient $c_1, \ldots, c_{k-1} \in \mathbb{N}$, et $p(x) := x^k - c_{k-1}x - \ldots - c_1 x - 1$. Si $\rho > 0$ est une racine rationnelle de $p(x)$, alors $\rho = 1$.*

Preuve. Écrivons $\rho = \frac{p}{q}$ avec $p, q \in \mathbb{N}^*$ et $\mathrm{pgcd}(p, q) = 1$. Alors, en utilisant le fait que ρ est une racine de $p(x)$, on obtient

$$p^k = c_{k-1}p^{k-1}q + c_{k-2}p^{k-2}q^2 + \ldots + c_1 pq^{k-1} + q^k$$

qui implique que p divise q. □

Enfin, il est nécessaire de pouvoir préciser les valeurs de b pour lesquelles la loi de Benford est satisfaite au moins lorsque les coefficients c_j sont rationnels.

Théorème 6. *Soit $(a_n)_{n\geq 1} \subset \mathbb{R}^+ \setminus \{0\}$ une suite qui satisfait la relation de récurrence d'ordre k*

$$a_{n+k} = c_{k-1}a_{n+k-1} + c_{k-2}a_{n+k-2} + \ldots + c_1 a_{n+1} + c_0 a_n$$

avec des coefficients $c_i \geq 0$, $c_0 > 0$ et $\{i < k : c_i > 0\} \neq \emptyset$, et avec les valeurs initiales $a_1, \ldots, a_k$ strictement positives. Alors :

(1) *La suite $(a_n)_{n\geq 1}$ satisfait la loi de Benford dans presque toute base b au sens suivant :*

$$\lim_{N\to\infty} \frac{1}{N} |\{2 < b \leq N : (a_n) \text{ ne suit pas la loi de Benford en base } b\}| = 0.$$

(2) *Si les coefficients c_i sont tous rationnels et si la racine réelle positive du polynôme caractéristique de la relation de récurrence n'est ni un entier ni un inverse d'entier, alors $(a_n)_{n\geq 1}$ satisfait la loi de Benford dans toute base $b > 2$.*

Remarque. Dans le cas où seul $c_0 > 0$, c'est-à-dire si $I = \emptyset$, toute suite $(a_n)_{n\geq 1}$ qui satisfait la relation de récurrence $(\star)$ est de la forme :

$$a_n = (\sqrt[k]{c_0})^n \cdot \sum_{\ell=0}^{k-1} \alpha_\ell e^{2\pi i \ell n/k} \quad \forall n.$$

Par pédiodicité de $e^{2\pi i \ell n/k}$, la suite (a_n) est donc réunion de k sous-suites $(a_{m+kn})_{n\geq 1}$, $0 \leq m < k$, qui sont toutes géométriques de raison c_0.

Ainsi, si $c_0 \neq 1$, chaque sous-suite $(a_{m+kn})_{n\geq 1}$ satisfait la loi de Benford dans presque toute base. Si en revanche $c_0 = 1$, chaque sous-suite est constante et ne satisfait pas la loi de Benford.

Les preuves utilisent principalement la matrice compagnon du polynôme $p(x)$ et elles reposent sur la théorie de Perron-Frobenius des matrices à coefficients positifs ou nuls qui sont irréductibles ou primitives, et dont nous rappelons les principaux résultats dans le paragraphe suivant. Les preuves des théorèmes 2 et 3 se trouvent dans le paragraphe 3 et la preuve du théorème 6 dans le dernier paragraphe.

2 Matrices irréductibles ; matrices primitives

Nous rappelons ci-dessous les définitions et les résultats principaux de la théorie de Perron-Frobenius à propos des matrices irréductibles et primitives. Nos références sont d'une part le chapitre 8 de la monographie de Carl D. Meyer [7] et d'autre part les notes de J.E. Rombaldi [8].

Soit $C \in M_k(\mathbb{R})$ une matrice $k \times k$ à coefficients positifs ou nuls (on note $C \geq 0$). Nous considérerons ici les valeurs propres complexes de C, c'est-à-dire ses valeurs propres en tant qu'endomorphisme de $\mathbb{C}^k$. L'ensemble des valeurs propres est le *spectre* de C et sera noté $\sigma(C)$. Nous rappelons que le *rayon spectral* de C est

$$\rho(C) = \max\{|\lambda| : \lambda \in \sigma(C)\}.$$

On dit que C est *réductible* s'il existe une matrice de permutation P telle que PCP^{-1} soit de la forme :

$$PCP^{-1} = \begin{pmatrix} C' & C''' \\ 0 & C'' \end{pmatrix}$$

où C' et C'' sont des matrices carrées de dimensions positives, et on dit qu'elle est *irréductible* si elle n'est pas réductible.

On démontre qu'une telle matrice $C = (c_{i,j})$ est irréductible si et seulement si le *graphe orienté* $G(C)$ associé est fortement connexe. Le graphe $G(C)$ a pour ensemble de sommets les entiers $1, 2, \ldots, k$, et il y a une arête *orientée* de i vers j si et seulement si $c_{i,j} > 0$; le graphe est *fortement connexe* s'il existe un chemin orienté de 1 vers 1 passant par tous les sommets.

Si C est irréductible, le rayon spectral $\rho = \rho(C)$ est strictement positif et c'est une valeur propre simple du polynôme caractéristique $p_C(x) = \det(C - xI)$. Le sous-espace propre correspondant est de dimension (complexe) égale à 1, et il est engendré par un *vecteur de Perron-Frobenius*, c'est-à-dire un vecteur $v = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$ dont toutes les composantes v_i sont strictement positives.

Notons $h \geq 1$ le nombre de valeurs propres $\lambda \in \sigma(C)$ telles que $|\lambda| = \rho$. Si $h > 1$, on l'appelle *l'indice d'imprimitivité* de C, et si $h = 1$, on dit que C est *primitive*.

On démontre que si C est irréductible, alors elle est primitive si et seulement s'il existe un entier $m > 0$ tel que $C^m > 0$, c'est-à-dire les coefficients de C^m sont tous strictement positifs (test de primitivité de Frobenius, cf. [7, pp. 674 et 678]).

Si C est irréductible mais non primitive, si $\{\lambda_1, \ldots, \lambda_h\}$ est l'ensemble des valeurs propres de C de module égal à ρ, alors

$$\{\lambda_1, \ldots, \lambda_h\} = \{\rho, \rho\omega, \rho\omega^2, \ldots, \rho\omega^{h-1}\}$$

où $\omega = e^{2\pi i/h}$ ([7, p. 676]).

Soit $S = (s_{i,j}) \in M_k(\mathbb{R})$ une matrice à coefficients positifs ou nuls. On dit que S est *stochastique* (par rapport aux lignes) si, pour tout $1 \leq i \leq k$, on a

$$\sum_{j=1}^{k} s_{i,j} = 1.$$

Si une telle matrice S est de plus irréductible, si h est son indice d'imprimitivité, alors elle admet toutes les racines h-ième de l'unité comme valeurs propres.

Grâce au test de primitivité de Frobenius, on observe que si A et B sont des matrices à coefficients positifs ou nuls irréductibles et s'il existe $\epsilon > 0$ tel que $A \geq \epsilon B$ (c'est-à-dire si $a_{i,j} \geq \epsilon b_{i,j}$ pour tous i, j), alors A est primitive si B l'est.

Considérons encore une matrice $C \geq 0$ irréductible et notons $v = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix} > 0$ un vecteur de Perron-Frobenius de C ; la transposée C^T de C possède les mêmes propriétés, donc elle admet un vecteur de Perron-Frobenius $w = \begin{pmatrix} w_1 \\ \vdots \\ w_k \end{pmatrix} > 0$ associé également au rayon spectral ρ.

Si de plus C est primitive, alors la suite de matrices $(\frac{1}{\rho^n} C^n)_{n \geq 1}$ converge vers la matrice $G := vw^T / w^T v$ qui est la projection sur le noyau de $C - \rho I$ parallèlement à l'image de $C - \rho I$ ([7, p. 674]). On observe que G a tous ses coefficients strictement positifs.

3 Preuves des théorèmes 2 et 3

Considérons d'abord un polynôme $p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0$ comme dans la première partie du théorème 2, c'est-à-dire tel que $c_j \geq 0$ pour tout $1 \leq j \leq k-1$ et $c_0 > 0$. On lui associe sa *matrice compagnon*

$$C = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ c_0 & c_1 & \ldots & c_{k-2} & c_{k-1} \end{pmatrix}.$$

Cela signifie que le polynôme caractéristique $p_C(x) = \det(C - xI)$ satisfait : $p_C(x) = (-1)^k p(x)$. Les deux polynômes ont par conséquent exactement les mêmes racines avec les mêmes multiplicités. Comme $c_0 > 0$, C est irréductible puisque, dans le graphe associé, il y a une arête de 1 vers 2, de 2 vers 3, etc. de $k-1$ vers k et de k vers 1, au moins. Ainsi, $p(x)$ satisfait les conditions de la première partie du théorème 2 si et seulement si sa matrice compagnon est primitive.

La partie (1) du théorème 2 est alors une conséquence immédiate de la proposition 7 ci-dessous, qui est un cas particulier du théorème de la page 679 de [7], mais nous en donnons une démonstration par souci d'être complet.

Proposition 7. *Soient $c_0, c_1, \ldots, c_{k-1}$ des nombres réels positifs ou nuls, $c_0 > 0$ et soit $I = \{1 \leq j < k : c_j > 0\}$. Alors la matrice*

$$C = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ c_0 & c_1 & \ldots & c_{k-2} & c_{k-1} \end{pmatrix}$$

est primitive si et seulement si $\mathrm{pgcd}(I \cup \{k\}) = 1$.

Preuve. Comme nous l'avons observé ci-dessus, C est irréductible. Notons N le cardinal de I. Soit S la matrice

$$S = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ \frac{1}{N+1} & \cdots & \frac{1}{N+1} & \cdots & \frac{1}{N+1} \end{pmatrix}$$

où dans la dernière ligne, pour tout $j \in I \cup \{0\}$, c_j est remplacé par $\frac{1}{N+1}$. La matrice ainsi obtenue est donc stochastique. En particulier, $\rho(S) = 1$, et S est irréductible. De plus, par

les rappels du paragraphe 2, C est primitive si et seulement si S l'est. On remplace alors C par S, qui est la matrice compagnon de

$$q(x) = x^k - \sum_{j \in I \cup \{0\}} \frac{x^j}{N+1}.$$

Supposons d'abord que $d = \operatorname{pgcd}(I \cup \{k\}) > 1$. Écrivons $j = a_j d$ et $k = ad$ avec $a_j, a \in \mathbb{N}^*$ pour tout $j \in I$, et considérons le polynôme

$$r(x) = x^a - \sum_{j \in I \cup \{0\}} \frac{x^{a_j}}{N+1}.$$

Alors $q(x) = r(x^d)$, $r(1) = 0$, et pour tout $\zeta \in \mathbb{C}$, $\zeta^d = 1$, on a $q(\zeta) = r(1) = 0$. Cela démontre que C n'est pas primitive.

Réciproquement, supposons que $\operatorname{pgcd}(I \cup \{k\}) = 1$, et soit ζ une racine de $q(x)$ telle que $|\zeta| = 1$. Par le paragraphe 2, on sait que ζ est alors une racine de l'unité. Écrivons donc

$$\zeta = e^{2i\pi m/d}$$

avec $1 \leq m \leq d$ et $\operatorname{pgcd}(m, d) = 1$. L'égalité $q(\zeta) = 0$ donne

$$(N+1)e^{2i\pi km/d} = \sum_{j \in I} e^{2i\pi jm/d} + 1,$$

et en prenant les modules

$$N + 1 = \Big| \sum_{j \in I} e^{2i\pi jm/d} + 1 \Big| \leq \sum_{j \in I} |e^{2i\pi jm/d}| + 1 = N + 1$$

qui implique que d divise jm pour tout $j \in I$, donc que $e^{2i\pi jm/d} = 1$, puis que $e^{2i\pi km/d} = 1$, donc que d divise également km. Ces conditions impliquent que d divise $\operatorname{pgcd}(I \cup \{k\})$; comme $\operatorname{pgcd}(m, d) = 1$, on obtient que $\zeta = 1$, et S est primitive. □

Pour démontrer la seconde affirmation du théorème 2, considérons un polynôme à coefficients réels $p(x) = x^k - cx^{k-1} - \sum_{j=0}^{k-2} c_j x^j$ tel que $c \geq 2$ et $c > \sum_{j=0}^{k-2} |c_j| + 1$. On observe d'abord que pour tout $z \in \mathbb{C}$ tel que $|z| \geq 1$, on a

$$\Big| \sum_{j=0}^{k-2} c_j z^j \Big| < |z|^{k-2}(c-1).$$

Cela implique facilement que $p(c-1) < 0$, que $p(c+1) > 0$ et que $p(z) \neq 0$ pour tout $|z| = 1$. Ainsi, p s'annule en un nombre réel $1 \leq c - 1 < \rho < c + 1$. Enfin, soit $q(z) = z^k - cz^{k-1}$. On a $|q(z)| \geq c - 1$ pour tout $|z| = 1$, et, pour ces mêmes valeurs de z, on a

$$|p(z) - q(z)| = \Big| \sum_{j=0}^{k-2} c_j z^j \Big| < c - 1 \leq |q(z)|.$$

Puisque q admet $k-1$ zéros (comptés avec multiplicités) dans le disque unité ouvert, il en est de même pour p par le théorème de Rouché. □

Considérons ensuite une suite $(a_n)_{n\geq 1}$ comme dans la troisième partie du théorème 2 : $a_n > 0$ pour tout n, et elle satisfait la relation de récurrence

$$a_{n+k} = c_{k-1}a_{n+k-1} + c_{k-2}a_{n+k-2} + \ldots + c_1 a_{n+1} + c_0 a_n \quad (n \geq 1)$$

où les c_i satisfont l'une des deux premières conditions du théorème 2. On note encore ρ l'unique racine positive du polynôme caractéristique $p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0$ de la relation de récurrence.

Pour démontrer la troisième partie du théorème 2, il suffit de vérifier que $\lim_{n\to\infty} \frac{a_n}{\rho^n}$ existe et est positive ([5, théorème 2.4]). Le cas où les coefficients c_i satisfont la condition (1) est une conséquence de la proposition suivante.

Proposition 8. *Avec les hypothèses et les notations ci-dessus, si les c_i satisfont la condition* (1) *du théorème* 2*, on a :*

$$\lim_{n\to\infty} \frac{a_n}{\rho^n}$$

existe et est positive.

Preuve. Notons encore C la matrice compagnon du polynôme $p(x)$ et posons pour tout entier $n \geq 1$

$$A_n = \begin{pmatrix} a_n \\ a_{n+1} \\ \vdots \\ a_{n+k-1} \end{pmatrix}$$

de sorte que

$$CA_n = A_{n+1}$$

pour tout $n > 0$. Par suite, on a $A_n = C^{n-1}A_1$ pour tout n. Si v et w sont des vecteurs de Perron-Frobenius pour C et C^T respectivement, on a vu que la suite de matrices $(\frac{1}{\rho^n}C^n)$ converge vers la matrice $G = vw^T/w^T v$ lorsque $n \to \infty$. Ainsi,

$$\frac{1}{\rho^n}A_n = \frac{1}{\rho} \cdot \frac{1}{\rho^{n-1}}C^{n-1}A_1 \to_{n\to\infty} \frac{1}{\rho}GA_1.$$

En particulier, $\frac{a_n}{\rho^n}$, qui est la première composante de $\frac{1}{\rho^n}A_n$, converge vers la première composante de $\frac{1}{\rho}GA_1$, et comme $A_1 > 0$ et $G > 0$, toutes les composantes de GA_1 sont positives. □

Pour terminer la preuve du théorème 2, considérons une suite $(a_n)_{n\geq 1} \subset \mathbb{R}^+ \setminus \{0\}$ qui satisfait la relation de récurrence

$$a_{n+k} = c_{k-1}a_{n+k-1} + \ldots + c_1 a_{n+1} + c_0 a_n$$

avec $c_{k-1} \geq 2$, $c_{k-1} > \sum_{j=0}^{k-2} |c_j| + 1$, et telle que a_n ne converge pas vers 0 lorsque $n \to \infty$. D'après la structure de telles suites (rappelée dans le paragraphe 1), si $\zeta_1 = \rho > 1$, $\zeta_2, \ldots, \zeta_m$ sont les racines du polynôme caractéristique $p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0$, de multiplicités respectives $\mu_1 = 1, \mu_2, \ldots, \mu_m$, il existe des coefficients $\alpha_{j,\ell}$ tels que

$$a_n = \alpha_{1,1}\rho^n + \sum_{j=2}^{m} \sum_{\ell=0}^{\mu_j - 1} \alpha_{j,\ell} n^\ell \zeta_j^n \quad \forall n \geq 1.$$

Puisque $\rho > 1$ et $|\zeta_j| < 1$ pour tout $j = 2, \ldots, m$, a_n est de la forme $a_n = \alpha_{1,1}\rho^n + \beta_n$ avec $\beta_n \to 0$ lorsque $n \to \infty$. Les hypothèses $a_n > 0$ pour tout n et $a_n \not\to 0$ impliquent que $\alpha_{1,1} > 0$, et on obtient immédiatement que

$$\lim_{n\to\infty} \frac{a_n}{\rho^n} = \alpha_{1,1}. \qquad \square$$

Nous passons enfin à la preuve du théorème 3.

Preuve du théorème 3.. En n'écrivant que les coefficients non nuls dans l'expression du polynôme $p(x)$, on a

$$p(x) = x^k - c_{k-k_1}x^{k-k_1} - \ldots - c_{k-k_s}x^{k-k_s} - c_0$$

avec $1 \leq k_1 < \ldots < k_s < k$. Par le théorème de la page 679 de [7], on obtient :

$$h = \mathrm{pgcd}(k - k_1, \ldots, k - k_s, k) = \mathrm{pgcd}(k_1, \ldots, k_s, k) = \mathrm{pgcd}(I \cup \{k\}).$$

Écrivons, pour $1 \leq i \leq s$, $k_i = hk_i'$, et aussi $k = hk'$. Pour chaque m fixé, en remplaçant n par $m + hn$ dans la relation de récurrence, on obtient

$$a_{m+h(n+k')} = c_{k-k_1}a_{m+h(n+k'-k_1')} + \ldots + c_{k-k_s}a_{m+h(n+k'-k_s')} + c_0 a_{m+hn}.$$

Cela signifie que la suite $(a_{m+hn})_{n\geq 1}$ satisfait une relation de récurrence d'ordre k' dont le polynôme caractéristique $q(x)$ est

$$q(x) = x^{k'} - c_{k-k_1}x^{k'-k_1'} - \ldots - c_{k-k_s}x^{k'-k_s'}$$

avec $\mathrm{pgcd}(I(q) \cup \{k'\}) = 1$. On applique alors les conclusions des propositions précédentes à la suite $(a_{m+hn})_{n\geq 1}$. $\square$

4 Critère d'irrationnalité de $\log_b(\rho)$

Soit $p(x)$ le polynôme $p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_1 x - c_0$ avec $c_i \in \mathbb{R}^+$ et $c_0 > 0$. On désigne encore par I l'ensemble des indices $1 \leq i < k$ tels que $c_i > 0$, et par ρ la racine positive de $p(x)$. On suppose encore que $I \neq \emptyset$.

Le résultat suivant sera utilisé dans la preuve du théorème 6.

Proposition 9. *Soit $b > 2$ un entier. On suppose que les $c_i \in \mathbb{Q}^+$ et que :*

(1) $\mathrm{pgcd}(I \cup \{k\}) = 1$ *;*

(2) *ρ n'est ni entier, ni inverse d'entier.*

Alors $\log_b(\rho)$ *est irrationnel.*

Preuve. Supposons que $\log_b(\rho)$ soit rationnel, de sorte qu'il existe deux entiers p et $q > 0$ premiers entre eux tels que $\rho = b^{p/q}$. Comme $\rho \neq 1$, on a $p \neq 0$. Désignons par $m(x)$ le polynôme minimal (unitaire) de ρ.

Si ρ est irrationnel, alors $m(x)$ est de degré au moins 2 et ρ en est une racine simple. Mais ρ est également une racine de $t(x) = x^q - b^p$, donc le polynôme $m(x)$ divise $t(x)$, et ainsi toutes les racines de $m(x)$ sont des racines de $t(x)$. Or, ces dernières sont toutes de module égal à ρ. Cela contredit (1) car $m(x)$ divise également $p(x)$, et ce dernier aurait plusieurs racines de module égal à ρ.

Par suite, ρ est nécessairement rationnel ; il existe des entiers positifs α, β tels que $\rho = \frac{\alpha}{\beta}$ et $\mathrm{pgcd}(\alpha, \beta) = 1$. On obtient $\alpha^q = b^p \beta^q$, et l'unicité de la décomposition en facteurs premiers implique que

$\beta = 1$ si p est positif, c'est-à-dire si $\rho > 1$, et alors $\rho = \alpha$ est entier,
$\alpha = 1$ si p est négatif, c'est-à-dire si $\rho < 1$, et alors $\rho = 1/\beta$ est un inverse d'entier,

ce qui contredit la seconde hypothèse. □

Remarque. La condition (2) est facile à utiliser puisqu'il est commode de localiser ρ dans $\mathbb{R}^+$ grâce à une étude succinte du polynôme $p(x)$.

Exemple 10. Soit $m \geq 1$ un entier fixé ; pour tout entier $k \geq 2$, soit

$$p_{k,m}(x) = x^k - mx^{k-1} - mx^{k-2} - \ldots - mx - m,$$

qui généralise le polynôme caractéristique des suites de Fibonacci d'ordre k introduites dans l'exemple 4, et qui satisfait les conditions du théorème 2. Notons $\rho_{k,m}$ la racine positive de $p_{k,m}(x)$.

Elle est irrationnelle par la proposition 5, $\rho_{k,m} > 1$ car $p_{k,m}(1) = 1 - km < 0$, et en fait, $\rho_{k,m}$ est un *nombre de Pisot* (cf [2], [1]) : c'est un entier algébrique, et $p_{k,m}(x)$ est son polynôme minimal car on a $c_{k-1} \geq \ldots \geq c_0 > 0$, et toutes les racines $\zeta \neq \rho_{k,m}$ de $p_{k,m}(x)$ satisfont $|\zeta| < \rho_{k,m}$.

On a $m < \rho_{k,m} < m + 1$ car

$$p_{k,m}(m) = \begin{cases} 1 - k < 0, & m = 1, \\ \dfrac{m - m^k}{m - 1} < 0, & m \geq 2, \end{cases}$$

et $p_{k,m}(m + 1) = 1$ pour tout m.

Plus précisément, on va démontrer que $\rho_{k,m} < \rho_{k+1,m}$ pour tous k et m, et que

$$\frac{(m+1)k}{k+1} < \rho_{k,m} < m + 1$$

pour tout m et tout k assez grand. Cela démontrera que, pour tout m fixé, la suite $(\rho_{k,m})_{k\geq 2}$ est croissante et converge vers $m + 1$ lorsque $k \to \infty$.

La première affirmation provient des égalités :

$$p_{k+1,m}(\rho_{k,m}) = \rho_{k,m}^{k+1} - m\rho_{k,m}^{k} - \ldots - m\rho_{k,m} - m = \rho_{k,m} \cdot p_{k,m}(\rho_{k,m}) - m = -m$$

et $p_{k+1,m}(\rho_{k+1,m}) = 0$.

Pour démontrer la seconde affirmation, nous introduisons le polynôme auxiliaire

$$q(x) = (x-1)p_{k,m}(x) = x^{k+1} - (m+1)x^k + m.$$

On vérifie sans peine que

$$q\left(\frac{(m+1)k}{k+1}\right) = -\frac{m+1}{k+1}\left(\frac{(m+1)k}{k+1}\right)^k + m.$$

Or, l'inégalité $-\frac{m+1}{k+1}\left(\frac{(m+1)k}{k+1}\right)^k + m < 0$ est équivalente à $(m+1)^{k+1} > m(k+1)(1+1/k)^k$ qui est vraie dès que k est assez grand. Cela démontre la seconde affirmation.

Remarques.

(1) Les suites $(\rho_{k,m}^{\ell})_{\ell\geq 1}$ ne sont pas équidistribuées mod 1 car la distance entre $\{\rho_{k,m}^{\ell} : \ell \leq n\}$ et $\mathbb{N}$ tend vers 0. Mais qu'en est-il de $(\alpha \cdot \rho_{k,m}^{\ell})_{\ell\geq 1}$ pour α irrationnel positif ? (On sait que, pour presque tout nombre réel $x > 1$, la suite $(x^n)_{n\geq 1}$ est équidistribuée mod 1 ; cf. [6, chap.1, corollaire 4.2.])

(2) Si $c_0, c_1, \ldots, c_{k-1} \in \mathbb{Z}$ avec $k \geq 2$ sont tels que

$$c_{k-1} > \sum_{j=0}^{k-2} |c_j| + 1$$

et $c_0 \neq 0$, le polynôme associé $p(x) = x^k - c_{k-1}x^{k-1} - \ldots - c_0$ est le polynôme minimal d'un nombre de Pisot ρ_k ([1, chap. 5.2]), et cela donne une famille de suites qui satisfont une relation de récurrence à coefficients entiers non nécessairement positifs et qui satisfont également la loi de Benford d'après le théorème 2.

Nous passons enfin à la preuve du théorème 6 :

Preuve du théorème 6. (1) Pour $N \geq 3$ fixé, posons

$$B_N = \{2 < b \leq N : \log_b(\rho) \in \mathbb{Q}\}.$$

Il suffit de démontrer que

$$|B_N| \leq \frac{\sqrt{N}\log(N)}{\log(2)}.$$

C'est évident si B_N est vide ou s'il ne contient qu'un élément. S'il contient au moins deux éléments, soit $b_0 = \min\{b \in B_N\}$. Pour tout $b \in B_N$ tel que $b > b_0$, en utilisant encore la décomposition en facteurs premiers, on vérifie qu'il existe un entier $u \leq \sqrt{N}$ tel que b_0 et b soient des puissances entières de u. Par suite,

$$B_N \subset \{2 < u^p \leq N : p \geq 1, u \leq \sqrt{N}\}.$$

On obtient ainsi la majoration annoncée.

(2) Soit $h \geq 1$ le nombre de racines positives distinctes du polynôme $p(x)$. Les sous-suites qui ont des conditions initiales positives parmi $(a_{m+hn})_{n\geq 1}$, $0 \leq m < h$, ont un polynôme caractéristique dont $\rho^{1/h}$ est la racine positive. Si ρ n'est ni entier ni inverse d'entier, alors $\rho^{1/h}$ non plus et les conditions de la proposition 9 sont satisfaites.

Enfin, si ρ est rationnel, en utilisant la décomposition en facteurs premiers, on vérifie comme dans la preuve de la proposition 9 que $b^{\pm\alpha/\beta} \in \mathbb{N}$ pour des entiers positifs α et β. Par suite, il existe des entiers $c, d \geq 1$ et $u \geq 2$ tels que $\rho^{\pm 1} = u^c$ et $b = u^d$, mais alors ρ serait entier ou inverse d'un entier, contrairement à l'hypothèse. Cela démontre la deuxième partie du théorème 6. □

Références

[1] Bertin, M.-J. ; Decomps-Guilloux, A. ; Grandet-Hugot, M. ; Pathiaux-Delefosse, M. ; Schreiber, J.-P. : *Pisot and Salem numbers*. Birkhäuser Verlag, Basel 1992.

[2] Brauer, A. : On algebraic equations with all but one root in the interior of the unit circle. *Math. Nachr.* 4 (1951), 250–257.

[3] Diaconis, P. : The distribution of leading digits and uniform distribution mod 1. *Ann. Probab.* 5 (1977), 72–81.

[4] Jolissaint, P. : Loi de Benford, relations de récurrence et suites équidistribuées. *Elem. Math.*, 60 (2005), 10–18.

[5] Jolissaint, P. : Loi de Benford, relations de récurrence et suites équidistribuées II. *Elem. Math.* 64 (2009), 21–36.

[6] Kuipers, L. ; Niederreiter, H. : *Uniform distribution of sequences*. Dover Publications, Inc., Mineola, New York 2006.

[7] Meyer, C. : *Matrix Analysis and Applied Linear Algebra*. SIAM, Philadelphia 2000.

[8] Rombaldi, J.-E. : Matrices positives et irréductibles. `www-fourier.ujf-grenoble.fr/~rombaldi/AgregExterne/MatricesPositives.pdf`.

Hugues Deligny
Académie de La Réunion
20 rue Colbert
Saint Paul La Réunion
e-mail : `abozinis@hotmail.com`

Paul Jolissaint
Institut de Mathémathiques
Université de Neuchâtel
Emile-Argand 11
CH-2000 Neuchâtel, Suisse
e-mail : `paul.jolissaint@unine.ch`