Journal du groupe de recherche des étudiant(e)s en mathématiques de l'Université Laval

Septembre 2007

Avant-propos

Voici la première édition du journal publié par le groupe de recherche des étudiant(e)s en mathématiques de l'Université Laval. Ce groupe est formé d'étudiants qui sont récipiendaires d'une bourse de recherche de premier cycle (BRPC) du CRSNG (Conseil de recherches en sciences naturelles et en génie du Canada). Cette bourse nous a permis, pendant tout un été, d'être initié à la recherche universitaire. Toujours dans ce cadre, nous avons présenté, chacun à notre tour, notre sujet de recherche lors d'un court exposé ouvert à tous. Par la suite, l'idée nous est venue de mettre par écrit ces présentations. Ainsi, nous avons offert la possibilité à tous d'écrire un article qui résume leur travail.

Il est très important de souligner que cette recherche s'effectue sous la supervision d'un enseignant de l'université. Nous voulons donc remercier tous les professeurs associés à chaque étudiant pour leurs implications. De plus, nous désirons remercier le département de Mathématiques et Statistiques de l'Université Laval qui supporte financièrement ce journal.

Finalement, ce journal nous permet à tous de terminer en beauté un été formidable de recherche en mathématiques. Bonne Lecture !

Alexandre St-Onge
Rédacteur

Table des matières

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'Université Laval
Volume 1, septembre 2007, 5-8

L'image numérique

Jean-Sébastien Lévesque
superviseur : Jean-Jacques Gervais

Résumé

L'image numérique d'une matrice $A \in M_n(\mathbb{C})$ est définie par

$$W(A) = \{x^*Ax : x \in \mathbb{C}^n, \|x\| = 1\}$$

Cet ensemble contient les valeurs propres de A et est toujours borné, fermé et convexe. Cet article présentera certains cas particuliers, ainsi que la méthode dite classique pour calculer $W(A)$.

1 L'image numérique

Définition 1 *L'image numérique d'une matrice $A \in M_n(\mathbb{C})$, notée W(A), est l'ensemble des $\mu \in \mathbb{C}$ obtenus par le produit scalaire complexe $\langle Ax, x\rangle$ pour tout vecteur unitaire $x \in \mathbb{C}^n$.*

$$\begin{aligned} W(A) &= \{\langle Ax, x\rangle : x \in \mathbb{C}^n,\ \|x\| = 1\} \\ &= \{x^*Ax : x \in \mathbb{C}^n,\ x^*x = 1\} \end{aligned}$$

On remarque facilement que $\sigma(A) \subset W(A)$. En effet, en prenant $\lambda \in \sigma(A)$, on a alors $Ax = \lambda x$ pour un certain vecteur x que l'on supposera unitaire. En multipliant par x^* de chaque côté, on obtient $x^*Ax = \lambda$.

L'image numérique possède plusieurs propriétés géométriques intéressantes, mais également certaines propriétés que le spectre n'a pas. Par exemple, il n'y a aucun lien entre les spectres de deux matrices et le spectre de leur somme, alors qu'avec l'image numérique, on a $W(A+B) \subset W(A) + W(B)$.

2 Propriétés de l'image numérique

Voici quelques propriétés faciles à démontrer. Rappelons que $\|Ux\| = \|x\|$ et qu'une sous-matrice principale de A est obtenue en enlevant à la matrice A une ou plusieurs colonnes, ainsi que les lignes correspondantes.

1.	$W(U^*AU)$	$=$	$W(A)$	où U est unitaire ($U^*U = I$)
2.	$W(\alpha A + \beta I)$	$=$	$\alpha W(A) + \beta$	où $\alpha, \beta \in \mathbb{C}$
3.	$W(A')$	$\subset$	$W(A)$	où A' est une sous-matrice principale de A

L'image numérique d'une matrice est un ensemble non seulement borné et fermé, mais aussi convexe (et donc connexe). Ces particularités font en sorte qu'on peut s'intéresser uniquement à la frontière de l'image pour décrire celle-ci. De plus, les points non-différentiables de la frontière de $W(A)$ sont toujours des valeurs propres de la matrice A. Ces propriétés se remarquent facilement dans les exemples qui suivent.

3 Exemples

Voici quelques exemples d'image numérique. Les valeurs propres de chaque matrice ont également été ajoutées aux graphiques.

$$A = \begin{pmatrix} 1 & 2 \\ 0 & -1 \end{pmatrix} \qquad B = \begin{pmatrix} i & 2 & 0 \\ 0 & -i & 0 \\ 0 & 0 & 2 \end{pmatrix} \qquad C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & i & 0 \\ 0 & 0 & 0 & -i \end{pmatrix}$$

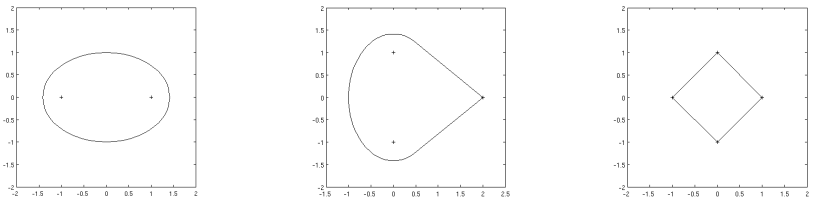


FIG. 1 – W(A), W(B) et W(C)

4 Quelques cas particuliers

4.1 Matrice 2x2

Par la propriété 1 et sans perte de généralité, posons

$$A = \begin{pmatrix} \lambda_1 & \alpha \\ 0 & \lambda_2 \end{pmatrix} \quad \text{où } \lambda_1, \lambda_2, \alpha \in \mathbb{C}$$

Théorème 1 *L'image numérique d'une matrice $A \in M_2(\mathbb{C})$ est une ellipse ayant pour foyers ses valeurs propres (λ_1 et λ_2) et un petit axe d'une longueur totale $|\alpha|$.*

Remarque : L'image ne sera pas nécessairement une véritable ellipse, mais elle correspondera toujours à l'idée d'une ellipse respectant les deux autres critères. Par exemple, $W(A)$ sera un segment si $|\alpha| = 0$, un cercle de diamètre $|\alpha|$ si $\lambda_1 = \lambda_2$ et un singleton si ces deux conditions sont réunis.

L'image numérique de l'exemple A de la section précédente est effectivement une ellipse ayant ces propriétés. On remarque également que les ellipses correspondant à chaque sous-matrice principale 2x2 de chacun des deux autres exemples sont contenues dans leur image numérique respective.

4.2 Matrice auto-adjointe ($H^* = H$)

Théorème 2 *L'image numérique d'une matrice auto-adjointe H (ou hermitienne) est le segment réel délimité par sa plus petite et sa plus grande valeur propre.*

$$W(H) = [\lambda_{min}, \lambda_{max}]$$

Preuve : Rappelons d'abord qu'une matrice hermitienne est toujours diagonalisable et que toutes ses valeurs propres sont réelles. Par la propriété 1, on peut prendre sans perte de généralité

$$H = \begin{pmatrix} \lambda_1 & 0 & \cdots & 0 \\ 0 & \lambda_2 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix} \text{ et posons } x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

où les $x_i \in \mathbb{C}$, $\|x\| = 1$, les $\lambda_i \in \mathbb{R}$ et supposons $\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$.

$[\lambda_1, \lambda_n] \subset W(H)$ se déduit facilement par la convexité de $W(H)$ et par le fait que $\sigma(H) \subset W(H)$. Pour $W(H) \subset [\lambda_1, \lambda_n]$, on développe x^*Hx et on remplace les λ_i par λ_1 ou par λ_n. On obtient alors $\lambda_1 \leq x^*Hx \leq \lambda_n$.

Ainsi, $W(H) \subset [\lambda_1, \lambda_n]$ et donc $W(H) = [\lambda_1, \lambda_n]$

□

4.3 Matrice normale ($A^*A = AA^*$)

Théorème 3 *L'image numérique d'une matrice normale est l'enveloppe convexe de son spectre, c'est-à-dire un polygone dont les sommets sont ses valeurs propres extrêmes.*

Il est clair que les sommets d'un polygone seront des valeurs propres, car ce sont des points non-différentiables sur $\partial W(A)$. L'exemple C de la section précédente correspond à l'image numérique d'une matrice normale.

5 Méthode classique de calcul

La méthode dite classique pour calculer $W(A)$ est basée sur la propriété de convexité et sur une décomposition de la matrice A en une somme de deux matrices hermitiennes. En posant

$$H = \frac{A + A^*}{2} \quad \text{et} \quad K = \frac{A - A^*}{2i}$$

on peut alors écrire A sous la forme $A = H + iK$. Il est facile de vérifier que $H^* = H$ et que $K^* = K$.

Lemme 1 *Si H et K sont définies par rapport à A comme précédemment, alors*

$$Re((W(A)) = W(H) \quad et \quad Im(W(A)) = W(K)$$

Preuve : En posant $A = H + iK$, on obtient $x^*Ax = x^*Hx + ix^*Kx$. Ainsi, tout $a \in W(A)$ peut s'écrire $a = h + ik$, où $h \in W(H)$ et $k \in W(K)$. Puisque H et K sont hermitiennes, on sait par le théorème 2 que $h, k \in \mathbb{R}$.

$$\begin{aligned} Re(W(A)) &= Re(\{a : a \in W(A)\}) = \{Re(a) : a \in W(A)\} \\ &= \{Re(h + ik) : h + ik \in W(A), h \in W(H), k \in W(K)\} \\ &= \{h : h \in W(H)\} = W(H) \end{aligned}$$

La preuve est identique pour $Im(W(A)) = W(K)$.

□

La méthode classique pour calculer $W(A)$ consiste à trouver la plus grande valeur propre de H, disons λ_{max}, et le vecteur propre correspondant. Par le théorème 2 et le lemme 1, on sait que $\lambda_{max} = max\{W(H)\} = max\{Re(W(A))\}$. On trouve ainsi le point le plus à droite sur la frontière de $W(A)$.

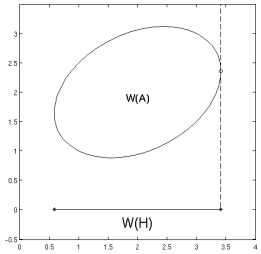


FIG. 2 – Méthode classique

Pour trouver d'autres points sur $\partial W(A)$, il suffit de faire tourner $W(A)$ d'un angle θ et de trouver le nouveau point le plus à droite de la même façon. Par la propriété 2, on peut faire tourner $W(A)$ en multipliant A par $e^{i\theta}$, car $W(e^{i\theta}A) = e^{i\theta}W(A)$. En prenant suffisamment d'angles $\theta_1 < \theta_2 < \cdots < \theta_k$ sur $[0, 2\pi]$, on obtient la frontière de $W(A)$.

Références

[1] N. Brassard, *L'image numérique*, Université Laval, 2003

[2] P. J. Psarrakos, M. J. Tsatsomeros, *Numerical range : (in) a matrix nutshell*, 2002

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 9-13

GREMUL

Règle de quadrature numérique sur une section polynômiale

Benoît Pouliot
superviseur : André Fortin

1 Introduction

Lorsque l'on utilise des méthodes numériques, il arrive souvent que l'on doive intégrer des milliers de fois des fonctions très complexes.

La quadrature de Gauss Legendre nous permet d'intégrer une fonction $f(x)$ sur un domaine $[-1, 1]$ en évaluant f qu'en seulement quelques points.

Le principe est simple : Trouvons les points x_i et les poids ω_i tels que

$$\int_{-1}^{1} f(x)dx \cong \sum_{i=1}^{N} \omega_i f(x_i)$$

soit exacte lorsque f est un polynôme d'ordre le plus élevé possible.

En théorie, on sait que l'ordre le plus élevé possible est 2N-1. Si on veut calculer exactement l'intégrale d'un polynôme d'ordre n, il faut alors prendre $\lceil \frac{n+1}{2} \rceil$ points et poids de Gauss. ($\lceil, \rceil$ indiquent l'entier supérieur ou égal)

De plus, il faut résoudre $n + 1$ équations pour trouver les points et poids de Gauss nécessaires :

$$\int_{-1}^{1} x^k dx = \sum_{i=1}^{\lceil \frac{n+1}{2} \rceil} \omega_i x_i^k \qquad \forall k \in \{0, 1, ..., n\}$$

Par contre, on sait qu'il existe des algorithmes très efficaces utilisant les zéros des polynômes de Legendre pour évaluer ces points rapidement.

Le problème sur lequel on va se pencher est de trouver les points et les poids de Gauss Legendre correspondant lorsque notre domaine n'est pas simple. Par exemple, la section polynômiale comprise entre $x = 0$, $y = 0$ et $x = (1 - y)^N$.

De plus, lorsque $N = 1$ on retrouve le triangle.

2 Motivations

Il faut d'abord vérifier que l'on peut utiliser les points et les poids de Gauss en deux dimensions.

Or, pour intégrer une fonction $f(x, y)$ sur un domaine fermé $[-1, 1]^2$, on peut quadriller notre domaine avec les points de Gauss obtenus en $1D$.

Ainsi, on s'assure d'obtenir la quadrature exacte jusqu'à l'ordre n.

Démonstration sur un polynôme P(x,y) d'ordre n.

$$\int_{\text{Carré}} P(x,y)dxdy = \int_{-1}^{1}\int_{-1}^{1} P(x,y)dxdy =$$

$$\sum_{n_k,m_k\leqslant n} \int_{-1}^{1}\int_{-1}^{1} A_k x^{n_k} y^{m_k} dxdy = \sum_{n_k,m_k\leqslant n} A_k \left[\int_{-1}^{1} x^{n_k}dx \int_{-1}^{1} y^{m_k}dy\right] =$$

$$\sum_{n_k,m_k\leqslant n} A_k \left[\sum_{i=1}^{N}\omega_i (x_i)^{n_k} \sum_{l=1}^{N}\omega_l (x_l)^{m_k}\right] = \sum_{n_k,m_k\leqslant n} A_k \left[\sum_{i=1}^{N}\sum_{l=1}^{N}\omega_i\omega_l (x_i)^{n_k}(x_l)^{m_k}\right] =$$

$$\sum_{i=1}^{N}\sum_{l=1}^{N}\omega_i\omega_l P(x_i,x_l) = \sum_{m=1}^{N^2}\omega_m P(x_m,y_m)$$

Ainsi, on se rend compte que l'intégration sur le carré sera exacte pour tous les polynômes du type $\sum_{n_k,m_k\leqslant n} A_k x^{n_k} y^{m_k}$. Cependant, il faut prendre $N^2 = \left\lceil \frac{n+1}{2} \right\rceil^2$ points.

On peut utiliser le même argument pour montrer que quadriller le cube $[-1, 1]^3$ par le même procédé rend aussi exacte l'intégration de polynômes de type $\sum_{n_k,m_k,o_k\leqslant n} A_k x^{n_k} y^{m_k} z^{o_k}$ sur ce dernier.

3 Procédé général

Puisqu'on a obtenu des points et des poids de Gauss en $2D$ et en $3D$, on va les utiliser sur d'autres géométries. Pour ce faire, on va introduire le changement de variable g correspondant.

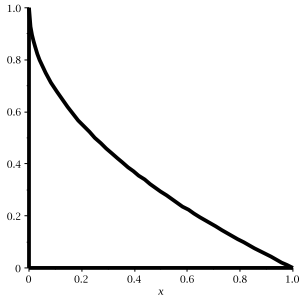
$$\int_{\text{Domaine 2D / Domaine 3D}} f(x)dE = \int_{\text{Carré / Cube}} f(g(x))|J|dE^*$$

Ici, J est le déterminant de la matrice Jacobienne du changement de variable.

Ainsi, on remarque que si $g(x)$ et $|J|$ sont des polynômes, on peut s'arranger pour trouver des points et des poids de Gauss en quadrillant encore une fois notre carré ou notre cube.

4 Section polynômiale

Dans cet article, on va se limiter à la section polynômiale décrite plus haut : $x = 0$, $y = 0$ et $x = (1-y)^N$, $(N \geq 1)$.



$$I = \int_0^1 \int_0^{1-\sqrt[N]{x}} f(x,y)dydx = \int_0^1 \int_0^{(1-y)^N} f(x,y)dxdy$$

Posons :

$$x = \left(\frac{1+\beta}{2}\right)^N, \qquad y = \frac{(1-\beta)(1+\alpha)}{4}$$

Alors :

$$dydx = |J|d\beta d\alpha = \left|\frac{\partial(x,y)}{\partial(\beta,\alpha)}\right| d\beta d\alpha = \frac{N(1-\beta)}{8}\left(\frac{1+\beta}{2}\right)^{N-1} d\beta d\alpha$$

Donc, on obtient :

$$I = \int_0^1 \int_0^{1-\sqrt[N]{x}} f(x,y)dydx$$

$$= \int_{-1}^1 \int_{-1}^1 f\left(\left(\frac{1+\beta}{2}\right)^N, \frac{(1-\beta)(1+\alpha)}{4}\right) \frac{N(1-\beta)}{8}\left(\frac{1+\beta}{2}\right)^{N-1} d\beta d\alpha$$

$$= \sum_{i=1}^{N_1}\sum_{j=1}^{N_2} \omega_i\omega_j \frac{N(1-\beta_i)}{8}\left(\frac{1+\beta_i}{2}\right)^{N-1} f\left(\left(\frac{1+\beta_i}{2}\right)^N, \frac{(1-\beta_i)(1+\alpha_j)}{4}\right)$$

$$= \sum_{m=1}^{N_1 N_2} c_m f(x_m, y_m)$$

On se ramène ainsi à un problème déjà résolu. On peut même expliciter les nouveaux points et poids :

$$\begin{cases} x_m = \left(\frac{1+\beta_i}{2}\right)^N \\ y_m = \frac{(1-\beta_i)(1+\alpha_j)}{4} \\ c_m = \omega_i\omega_j \frac{N(1-\beta_i)}{8}\left(\frac{1+\beta_i}{2}\right)^{N-1} \end{cases}$$

On peut calculer les valeurs de N_1 et de N_2 nécessaires selon le degré que l'on veut atteindre pour la quadrature. Si l'on veut un degré $n \geq k + l$, on trouve :

$$I = \int_0^1 \int_0^{1-\sqrt[N]{x}} x^k y^l dy dx$$

$$= \int_{-1}^{1} \int_{-1}^{1} \left(\frac{1+\beta}{2}\right)^{kN} \frac{(1-\beta)^l (1+\alpha)^l}{4^l} \frac{N(1-\beta)}{8} \left(\frac{1+\beta}{2}\right)^{N-1} d\beta d\alpha$$

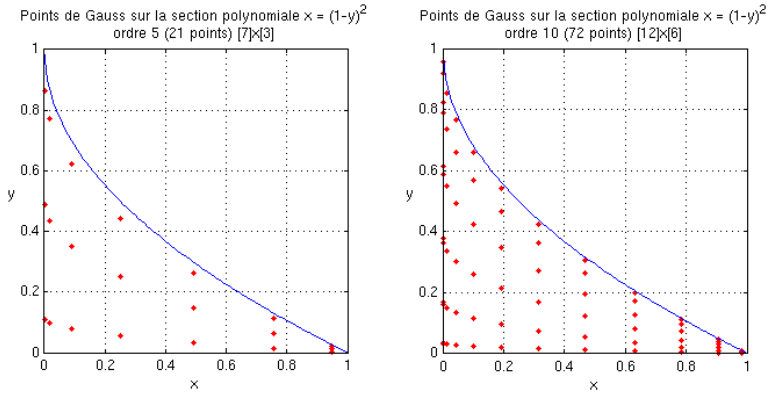
$$= \int_{-1}^{1} \sum_{i=0}^{kN+l+N} B_i \beta^i d\beta \int_{-1}^{1} \sum_{i=0}^{l} A_i \alpha^i d\alpha$$

Comme l'ordre maximal du premier polynôme est $N(n+1) \geq kN + l + N$, alors il faut prendre $N_1 = \left\lceil \frac{N(n+1)+1}{2} \right\rceil$.

Aussi, l'ordre maximal du second polynôme est $n \geq l$, alors $N_2 = \left\lceil \frac{n+1}{2} \right\rceil$

$$\begin{cases} N_1 = \left\lceil \frac{N(n+1)+1}{2} \right\rceil \\ N_2 = \left\lceil \frac{n+1}{2} \right\rceil \end{cases}$$

Donc, on a besoin de $\left\lceil \frac{N(n+1)+1}{2} \right\rceil \left\lceil \frac{n+1}{2} \right\rceil$ points et poids de Gauss pour la section polynômiale.

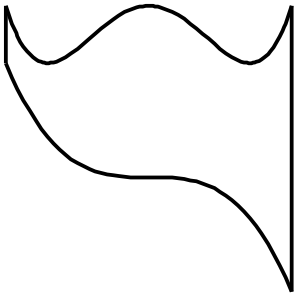


5 Conclusions

Le procédé énoncé ici est loin d'être optimal en terme de points dévaluation. En effet, il existe plusieurs autres règles de quadrature qui utilisent beaucoup moins de points x_i sur des domaines précis et ce pour atteindre les mêmes ordres de précision. Cependant, la règle décrite ici a quand même ses avantages : la génération des points et des poids est facile et rapide, l'utilisation de ces derniers est simple.

Sans l'expliciter ici, j'ai aussi trouvé les expressions pour calculer les points et poids de Gauss dans un cas un peu plus général. Lorsqu'on prend une section polynômiale quelconque : $x \in [x_0, x_1]$ et $y \in [p_0(x), p_1(x)]$.

$$I = \int_{x_0}^{x_1} \int_{p_0(x)}^{p_1(x)} f(x,y) dy dx$$



On pourrait aussi faire la même chose sur un domaine en trois dimensions.

Je tiens à souligner l'article de H. T. Rathod, B. Venkatesudu et K. V. Nagaraja (voir la référence) sur lequel je me suis basé pour faire cet article. En fait, ma règle de quadrature est une généralisation de leur règle de quadrature sur le tétraèdre.

Référence

H. T. Rathod, B. Venkatesudu et K. V. Nagaraja, Gauss Legendre Quadrature Formulas over a Tetrahedron, *Wiley InterScience*, (2005).

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 15-17

Survol de l'indice de composition des nombres $\lambda(n)$

Jean-Philippe Labbé
superviseur : Jean-Marie De Koninck

Résumé

L'*indice de composition* des nombres $\lambda(n)$ a été introduite en 2000 par Browkin. Par la suite Ribenboim l'a étudié en l'appelant *radical index of n*. L'article *À propos de l'indice de composition des nombres* de De Koninck et Doyon contient des propriétés élémentaires et une étude plus profonde de l'indice de composition. Finalement, de 2003 à ce jour, De Koninck, Kátai, Luca, et Subbarao ont collaboré dans plusieurs articles qui concernent cette fonction.

Introduction

Suite à mon premier stage en théorie des nombres et au cours d'introduction à la théorie analytique des nombres, je pouvais maintenant étudier l'indice de composition des nombres plus en détails. Pour commencer la recherche, je devais apprendre beaucoup sur ce sujet en me familiarisant avec la littérature existante. La compréhension du sujet étant très importante, cette dernière partie a pris une place prépondérante cet été. Par la suite, je devais rassembler et possiblement améliorer les connaissances sur l'indice de composition à travers la rédaction d'un article survolant le sujet. Voici donc l'indice de composition en un coup d'oeil.

L'indice de composition

Définitions et propriétés

En premier lieu, voici quelques définitions et conventions importantes. Étant donné un entier $n \geq 2$, nous définissons son *indice de composition* par $\lambda(n)) := \frac{\log n}{\log \gamma(n)}$ (de façon équivalente $\gamma(n)^{\lambda(n)} = n$), où $\gamma(n)$ (souvent appelé le *noyau* de n) représente le produit des premiers distincts qui divisent n. Par commodité, nous notons $\lambda(1) = \gamma(1) = 1$. Alors $\lambda(n) \geq 1$ pour tout entier $n \geq 1$. D'une certaine façon, $\lambda(n)$ mesure la multiplicité des facteurs premiers de n. Ainsi, un entier $n > 1$ est d'indice de composition supérieur à 1 si et seulement s'il n'est pas libre de carrés. Par ailleurs, les nombres k-puissants (i.e. les nombres $n > 1$

tels que $p^k|n$ pour chaque diviseur premier p de n), ont un indice de composition $\geq k$. Par convention, le nombre 1 est k-puissant pour chaque $k \geq 2$. De plus, les nombres 2-puissants sont simplement appelés puissants. Maintenant voici quelques propriétés de l'indice de composition.

- Soit un entier $k \geq 2$, tout entier non-nul n peut être représenté de façon unique sous la forme $n = \omega_k(n) \cdot n'$ où $\omega_k(n)$ est k-puissant, $pgcd(\omega_k(n), n') = 1$ et si $p|n'$ alors $p^k \not| n'$. Nous appelons $\omega_k(n)$ la partie k-puissante de n (pour $k = 2$, $\omega_k(n)$ est appelée partie puissante de n et n' la partie libre de carrée) ;
- Soit un entier $k \geq 1$, alors $\lambda(n^k) = k\lambda(n)$ pour chaque entier $n > 1$;
- L'indice de composition d'un nombre est un entier ou un nombre irrationel ;
- Si $\lambda(n) = \lambda(m)$ n'est pas un entier, alors $n = m$.
- L'ensemble $\{\lambda(n) : n = 1, 2, \ldots\}$ est dense dans l'ensemble des nombres réels ≥ 1.

Résultats sur l'indice de composition

Finalement, voici quelques résultats présents dans l'article de De Koninck et Doyon [3] avec lesquels j'ai dû travailler. La valeur moyenne asymptotique de $\lambda(n)$ et de $1/\lambda(n)$ a premièrement été étudiés par De Koninck et Doyon et améliorés par De Koninck et Kátai [5]. Dernièrement, W. Zhai [7] a généralisé les résultats trouvés précédemment.

Voici les premiers résultats obtenus

Théorème 1 *La valeur moyenne asymptotique de la fonction λ est 1. Plus précisément, lorsque $x \to \infty$, on a*

$$\sum_{n \leq x} \lambda(n) = x + c\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right),$$

avec $c = \sum_p \frac{\log p}{p(p-1)} \approx 0.75536$, où la somme infinie parcourt tous les nombres premiers p.

Le comportement local de $\lambda(n)$ a premièrement été caractérisé par

Théorème 2 *Pour tout entier $k \geq 2$ et tout $\epsilon > 0$, il existe une infinité d'entiers positifs n tels que*

$$Q_k(n) := \min(\lambda(n), \lambda(n+1), \ldots, \lambda(n+k-1)) > \frac{k}{k-1} - \varepsilon.$$

Il est possible de faire un lien avec la conjecture-ABC à l'aide du dernier théorème. En effet, dans [4], ils montrent que la conjecture-ABC impliquent que $\limsup_{n\to\infty} Q_k(n) = k/(k-1)$. En terminant, voici un résultat que nous avons obtenu à partir d'un lemme de [3].

Théorème 3 *Soit $A := \{(m,n) \in \mathbb{N}^2 : \lambda(m)\lambda(n) \leq \lambda(m) + \lambda(n)\}$ et notons $A(x) := \{(m,n) \in A : m, n \leq x\}$. La densité asymptotique de l'ensemble A est égale à 1. C'est-à-dire,*

$$\lim_{x\to\infty} \frac{\#A(x)}{x^2} = 1.$$

Conclusion

En quelques mots, durant ce stage de recherche en théorie des nombres, j'ai pu approfondir mes connaîssances sur le sujet et y connaître mes forces et faiblesses. Il est impossible de quantifier les notions que j'ai apprises ; non seulement on acquiert beaucoup de notions théoriques, mais on apprend aussi à communiquer oralement et à travers des textes, à travailler en équipe et on exerce notre autonomie. Finalement, un stage en recherche nous permet de se connaître davantage et de connaître un nouveau milieu différent d'une salle de classe.

Remerciements. Je tiens à remercier Nicolas Doyon, Quentin Rajon et Érik Pronovost pour avoir gentiment répondu à mes questions durant l'été et spécialement Jean-Marie De Koninck pour ses encouragements et sa disponibilité pour ma recherche malgré plusieurs projets.

Références

[1] J. Browkin, The abc-conjecture, dans "Number Theory", Trends Math. (2000), 75-105, Birkhäuser Basel.

[2] P. Ribenboim, The ABC conjecture and the radical index of integers, Acta Arithmetica, 96 (2001), 389-404.

[3] J.M. De Koninck et N. Doyon, À propos de l'indice de composition des nombres. Monatshefte für Mathematik, 139 (2003), 151-167.

[4] J.M. De Koninck et F. Luca, On the index of composition of the Euler function and of the sum of divisors function, Colloq. Math., 108 (2007), no. 1, 3151.

[5] J.M. De Koninck et I. Kátai, On the mean value of the index of composition of an integer, Monatshefte für Mathematik, 145 (2005), 131-144.

[6] J.M. De Koninck, I. Kátai et M.V. Subbarao, On the index of composition of integer from various sets, Archiv der Mathematik, 88 (2007), 524-536.

[7] W. Zhai, On the mean value of the index of composition of an integer, Acta Arithmetica. 125 (2006), no. 4, 331-345.

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 19-23

Les fractions continues, un classique ?

Alexandre St-Onge
superviseure : Line Baribeau

Résumé

L'étude des fractions continues est un classique dans la théorie des nombres mais un sujet d'actualité dans l'analyse complexe. Dans cet article, nous expliciterons le lien important reliant ces fractions à l'analyse complexe. Par la suite, nous introduirons certaines fonctions bien connues et essentielles à notre travail, les transformations de Möbius. Finalement, nous verrons, grâce à ces transformations, comment un théorème classique peut être généralisé.

1 Introduction

Tout d'abord, il est essentiel d'avoir une définition formelle des fractions continues. Voici celle que nous utilisons :

Définition 1. Une **fraction continue** est une fraction de la forme

$$\cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \ddots}} \tag{1}$$

où $a_n,\ b_n \in \mathbb{C}$ et $a_n \neq 0$ pour tout $n \geq 1$.

Voici un exemple classique et simple d'une telle fraction :

$$\cfrac{1}{1 + \cfrac{1}{1 + \ddots}}$$

Si nous dénotons par α la valeur de cette fraction continue, en remarquant que $\alpha = \frac{1}{1+\alpha}$, on trouve facilement que $1 + \alpha = \frac{1+\sqrt{5}}{2}$ qui est le célèbre nombre d'or. Ce ne sont cependant pas toutes les fractions continues qui convergent. Le but principal est donc de trouver des critères de convergence pour ces fractions.

En ce qui concerne le présent article, je veux vous exposer comment l'analyse complexe est liée aux fractions continues et vous montrer la généralisation d'un critère de convergence. Pour réussir tout cela, il nous faut premièrement une définition de la convergence.

Définition 2. La k-ième **réduite** d'une fraction continue (1) est définie comme

$$C_k \;=\; \frac{a_1}{b_1 + \ddots + \dfrac{a_k}{b_k}}.$$

Définition 3. La fraction continue (1) **converge** si et seulement si la suite des réduites, $(C_k)_{k\geq 1}$ converge.

2 Analyse complexe et transformations de Möbius

Pour découvrir le lien important entre l'analyse complexe et les fractions continues, nous commençons par prendre des fonctions complexes appropriées.
Posons $\forall\ n \in \mathbb{N}$,

$$s_n(z) \;=\; \frac{a_n}{b_n + z}.$$

Nous pouvons alors écrire les réduites d'une fraction continue (1) comme

$$C_k \;=\; s_1 s_2 \cdots s_k(0)$$

où $s_1 s_2 \cdots s_k$ est la composée $s_1 \circ s_2 \circ \cdots \circ s_k$. Donc, pour que la fraction continue converge, il faut que la suite $s_1 \cdots s_n(0)$ converge lorsque $n \longrightarrow \infty$.

Cette dernière remarque est peut-être la plus importante de cet article et il est essentiel de bien la comprendre. En effet, elle nous donne plusieurs libertés. Premièrement, nous pouvons penser aux démonstrations qui peuvent maintenant se situer dans l'analyse complexe. Deuxièmement, nous pouvons parler de convergence de la suite $s_1 \cdots s_n(z)$ et ce pour tout $z \in \mathbb{C}$ au lieu du seul point spécifique 0. Finalement, nous pouvons généraliser les fonctions s_n utilisées en parlant des transformations de Möbius. Avant d'étudier un exemple de critère de convergence généralisé, nous allons parler de ces tranformations et de leurs propriétés plus qu'intéressantes.

Définition 4. Une **transformation de Möbius** est une transformation de la forme

$$T(z) \;=\; \frac{az + b}{cz + d}, \quad ad - bc \;\neq\; 0.$$

Afin de bien travailler avec ces transformations, il nous faut nous placer dans un domaine approprié. Nous ajoutons à l'ensemble des complexes un point infini. Nous notons, $\mathbb{C}_\infty = \mathbb{C} \cup \{\infty\}$ et nous posons de façon naturelle $T(\infty) = a/c$ et $T(-d/c) = \infty$. Cela permet de considérer les transformations de Möbius comme des fonctions $T : \mathbb{C}_\infty \longrightarrow \mathbb{C}_\infty$ et ce point de vue est intéressant car elles deviennent des homéomorphismes. Donc, elles sont bijectives, continues et leurs inverses aussi. Enfin, il est possible de montrer que les transformations de Möbius ainsi définies transforment un cercle ou une droite en un cercle ou une droite.

3 Théorèmes de convergence

3.1 Théorème de Pringsheim

Alfred Pringsheim est un mathématicien allemand né en 1850 et mort en 1941. C'est en 1898 qu'il démontre le théorème suivant :

Théorème 1. *Suppossons que* $|b_n| \geq 1+|a_n|\,,\ \forall\, n$. *Alors, la fraction continue*

$$\cfrac{a_1}{b_1 + \cfrac{a_2}{b_2 + \ddots}}$$

converge vers une valeur, v, avec $|v| \leq 1$.

Bien qu'il soit très intéressant, ce résultat sur la convergence ne concerne que les fractions continues. Grâce à notre nouveau point de vue, nous pouvons tirer de l'information supplémentaire. En effet, prenons les transformations de Möbius

$$s_n(z) = \frac{a_n}{b_n + z}$$

et supposons que $|b_n| \geq 1+|a_n|\,,\ \forall\, n$. On sait que ces transformations envoient le cercle unité vers un autre cercle mais nous avons de plus que $s_n(\mathbb{D}) \subset \mathbb{D}$. Nous obtenons ensuite, lorque nous nous intéressons à la suite $s_1 \cdots s_n$, que

$$\mathbb{D} = s_1(\mathbb{D}) \supset s_1 s_2(\mathbb{D}) \supset s_1 s_2 s_3(\mathbb{D}) \supset \ldots.$$

Géométriquement, nous obtenons une suite de disques imbriqués les uns dans les autres. Il y a donc, derrière les hypothèses du théorème de Pringsheim, certains critères géométriques plus importants et ceci nous mènent à une généralisation : Le théorème de Hillam-Thron.

3.2 Théorème de Hillam-Thron

C'est en 1965 que Hillam et Thron ont démontré ce théorème.

Théorème 2. *Supposons que* $\mathbb{D} \subset \mathbb{C}$ *est le disque unité. Supposons aussi que, pour tout* $n \in \mathbb{N}$, s_n *sont des transformations de Möbius telles que* $s_n(\mathbb{D}) \subset \mathbb{D}$ *et* $s_n(\infty) = w$ *pour un* $w \in \mathbb{D}$. *Alors la suite* $s_1 s_2 \cdots s_n$ *converge localement uniformément sur* $\mathbb{D}$ *vers un point dans la fermeture,* $\bar{\mathbb{D}}$, *de* $\mathbb{D}$.

Avant tout, voyons comment le théorème 1 est une conséquence du théorème 2. Prenons les transformations de Möbius suivantes :

$$s_n(z) \;=\; \frac{a_n}{b_n + z}$$

et supposons qu'elles respectent l'hypothèse du théorème de Pringsheim, c'est-à-dire que $|b_n| \;\geq\; 1 + |a_n|$ pour tout $n \;\geq\; 1$.

Nous savons déjà que $s_n(\mathbb{D}) \;\subset\; \mathbb{D}$ et facilement, $s_n(\infty) \;=\; 0 \;\in\; \mathbb{D}$. Nous pouvons donc utiliser le théorème de Hillam-Thron pour conclure que la suite $s_1 \cdots s_n$ converge localement uniformément sur $\mathbb{D}$. Ainsi, $s_1 \cdots s_n(0) \;\longrightarrow\; v \;\in\; \bar{\mathbb{D}}$. Ceci implique que la fraction continue engendrée par ces transformations converge, ce qui est bien la conclusion du premier théorème.

Ensuite, j'aimrais vous convaincre que le théorème de Hillam-Thron est plus général que celui de Pringsheim. Premièrement, nous pouvons prendre des transformations de Möbius générales

$$s_n(z) \;=\; \frac{a_n z + b_n}{c_n z + d_n},$$

tandis que dans le premier théorème, nous nous limitons aux transformations de la forme

$$s_n(z) \;=\; \frac{a_n}{z + b_n}.$$

Deuxièmement, la conclusion du théorème de Hillam-Thron porte sur la convergence localement uniforme sur $\mathbb{D}$ de la suite $s_1 \cdots s_n$ plutôt que la convergence simple de $s_1 \cdots s_n(0)$. Il faut donc bien comprendre ce qu'est la convergence localement uniforme sur $\mathbb{D}$. Nous parlons donc de cette convergence lorsque, sur tout compact K de $\mathbb{D}$, la suite $s_1 \cdots s_n(0)$ converge uniformément sur K. Ainsi, cette convergence est plus forte que la convergence simple d'où le fait que la conclusion du deuxième théorème est plus forte que celle du premier.

4 Conclusion

Nous avons vu ici un seul exemple de généralisation dans l'analyse complexe de résultats sur les fractions continues, mais bien sûr ce n'est pas l'unique possibilité. Plusieurs autres théorèmes classiques sont étudiés grâce aux transformations de Möbius, comme par exemple le théorème de Stern-Stolz. De plus, les transformations de Möbius possèdent un fort caractère géométrique et grâce à ceci, il est possible, à partir de $\mathbb{C}_\infty$, d'étendre leurs actions à $\mathbb{R}^3$ et même à $\mathbb{R}^N$. De cette manière, il est possible de généraliser le concept des fractions continues pour des espaces de dimensions plus élevées. Par la même occasion, nous pouvons aussi étudier les fractions continues à l'aide de la géométrie hyperbolique et ce grâce aux espaces hyperboliques. La possibilité de trouver des démonstrations plus courtes ou des généralisations est donc certainement présente.

Pour terminer, j'ai adoré le sujet des fractions continues pour la simple et bonne raison que j'ai réussi à travailler dans l'analyse complexe, la géométrie hyperbolique et la dynamique complexe. Je tiens à remercier Line Baribeau pour cette chance et son aide dans tout ce travail.

Références

[1] A. F. Beardon, *Continued Fractions, Discrete Groups and Complex Dynamics*, Computational Methods and Function Theory Vol.1 (2001), 535-594.

[2] A. F. Beardon, *The Geometry of Pringsheim's Continued Fractions*, Geometriae Dedicata Vol.84 (2001), 125-134.

[3] A. F. Beardon, *The Hillam-Thron Theorem in Higher Dimensions*, Geometriae Dedicata Vol.96 (2003), 205-209.

[4] K. L. Hillam et W. J. Thron, *A General Convergence Criterion for Continued Fraction* $K(a_n|b_n)$, Proceedings of the American Mathematical Society Vol.16 (1965), 1256-1262.

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 25-28

Quelques problèmes sur les matrices de Hadamard

Jérôme Fortier
superviseur : Javad Mashreghi

Résumé

Une matrice de Hadamard est une matrice orthogonale à coefficients dans $\{\pm 1\}$. Outil utile en théorie du signal, en théorie du design et en cryptographie, elles sont d'abord un objet mathématique fort intéressant, à propos duquel même les questions les plus simples demeurent ouvertes. Cet article se veut un accès rapide aux énoncés de quelques problèmes de recherche, tous tirés du livre *Hadamard Matrices and their Applications* par K. J. Horadam, et le lecteur est référé en bibliographie pour plus de détails.

1 Définitions et propriétés

Définition 1 *Soit H une matrice carrée d'ordre n dont les coefficients sont uniquement dans $\{\pm 1\}$. Alors H est une* matrice de Hadamard *si elle satisfait*

$$HH^\top = nI_n$$

Autrement dit, si H est une matrice de Hadamard, alors le produit scalaire de deux rangées distinctes de la matrice est toujours égal à 0. L'on montre facilement que si H est Hadamard, alors $H^\top$ l'est également, et donc, cette propriété tient également pour les colonnes de H.

De plus, en multipliant une rangée (ou une colonne) de H par -1, ou en permutant deux ou plusieurs rangées (colonnes), on ne change pas la propriété du produit scalaire. On peut ainsi obtenir plusieurs matrices de Hadamard à partir d'une seule. On définit que deux matrices à coefficients dans $\{\pm 1\}$ sont *Hadamard-équivalentes* si l'une peut être obtenue à partir de l'autre par implémentation finie de ces deux dernières opérations. En outre, chaque matrice de Hadamard peut être *normalisée* en transformant sa première rangée et sa première colonne par seulement des 1.

Problème 1 *Quelle est la valeur du nombre $h(n)$ de classes d'équivalence de matrices de Hadamard d'ordre n, pour un n donné ($n \geq 32$) ? Quel est son comportement asymptotique lorsque $n \to \infty$? A-t-on $h(n) \leq h(2n)$ pour tout n ?*

Une première particularité des matrices de Hadamard est que s'il existe une matrice de Hadamard d'ordre n, alors $n = 1, 2$ ou $4t$ pour un $t \in \mathbb{N}$. Supposons en effet qu'il existe une matrice de Hadamard $H = [h_{ij}]$ d'ordre $n \geq 2$. On considére la comme S suivante, que l'on compte de deux façons pour obtenir $n = 4t$.

$$S = \sum_{k=1}^{n} (h_{1k} + h_{2k})(h_{1k} + h_{3k})$$

On aimerait toutefois savoir si la réciproque de ce théorème est vraie. Beaucoup d'indices laissent croire que oui. D'abord, le fait que nous connaissions des matrices de Hadamard d'ordre n pour beaucoup de multiples de 4 (avec comme seuls $n \leq 1000$ inconnus à ce jour : $668, 716$ et 892), et aussi par l'existence de résultats asymptotiques certifiant l'existence de matrices de Hadamard d'ordre $2^k m$ pour k assez grand en fonction de m. Malgré tout, il n'existe à ce jour aucune preuve de ce résultat simple mais fondamental.

Problème 2 (Conjecture de Hadamard) *Montrer que si n est un multiple de 4, alors il existe une matrice de Hadamard d'ordre n.*

Problème 3 *Construire une matrice de Hadamard d'ordre $668, 716$ ou 892.*

2 Généralisations

Il est naturel de se demander ce qu'il arrive lorsqu'on étend la définition d'une matrice de Hadamard à des objets plus généraux. En ce sens nous explorons des problèmes relatifs à trois types de géneralisations, que nous définissons ci-bas.

Définition 2 *Soit $D_m = \langle e^{2i\pi/m} \rangle$ le groupe des racines m-ièmes complexes de l'unité. Une matrice carrée H d'ordre n à coefficients dans D_m est une* matrice de Butson *de paramètres (m, n) si $H\overline{H}^\top = nI_n$.*

Dans les applications en théorie des communications, les cas $m = 2$ (les matrices de Hadamard) et $m = 4$ (les matrices quaternaires de Hadamard) sont les plus utilisées. Dans le cas quaternaire, il exste une conjecture semblable à celle de Hadamard, et qui implique cette dernière, car il existe une construction de matrices de Hadamard d'ordre $2n$ à partir de matrices quaternaires d'ordre n.

Problème 4 *Montrer que si n est pair, alors il existe une matrice quaternaire de Hadamard d'ordre n.*

Définition 3 *Soit G un groupe fini d'ordre m, et n un multiple de m. Une matrice carrée $H = [h_{ij}]$ d'ordre n est une* matrice généralisée de Hadamard *si, $\forall i \neq j$, la séquence $(h_{ik}h_{jk}^{-1})_{1 \leq k \leq n}$ contient tous les éléments de G exactement $\frac{n}{m}$ fois.*

Si G est abélien, et si H est une matrice généralisée de Hadamard, alors $H^\top$ en est également une. Rien n'indique qu'il en est ainsi dans le cas nonabélien, mais aucun exemple n'est connu.

Problème 5 *Trouver une matrice H généralisée de Hadamard telle que $H^\top$ n'en est pas une, ou montrer que celà est impossible.*

Problème 6 *Existe-t-il une matrice généralisée de Hadamard sur un groupe G d'ordre m, tel que m n'est pas un nombre premier ?*

Les matrices de Butson généralisent les applications des matrices de Hadamard à la théorie du signal et aux codes correcteurs d'erreurs, en permettant des alphabets de m caractères, tandis que l'autre généralisation sert d'outil à une théorie du design plus générale. Il est clair que l'intersection entre ces deux généralisations est loin d'être vide (elle contient au moins les matrices de Hadamard !), mais la question de caractériser cette intersection est encore ouverte.

Une matrice généralisée de Hadamard développée sur le groupe D_m est une matrice de Butson. Une matrice de Butson est dite *balancée* si sa version normalisée (analogue à la normalisation pour les matrices de Hadamard, avec multiplication par n'importe quel élément de D_m) contient sur chaque ligne et chaque colonne, sauf la première, tous les éléments de D_m exactement $\frac{n}{m}$ fois. Le résultat suivant est conjecturé quant à la caractérisation de l'intersection.

Problème 7 *Montrer qu'une matrice de Butson balancée est nécéssairement une matrice généralisée de Hadamard, ou trouver un contre-exemple.*

Enfin, le dernier type de généralisation des matrices de Hadamard que nous explorons ne porte pas sur le groupe des entrées de la matrice, mais sur la notion de matrice elle-même.

Définition 4 *Soit $k \geq 2$. Une* matrice de Hadamard d'ordre n à k dimensions *est un tenseur $H = [h(i_1, i_2, \ldots, i_k)]_{1 \leq i_j \leq n, \forall j}$ à coefficients dans $\{\pm 1\}$ tel que, pour tout $1 \leq l \leq k$, et pour des indices x et y fixés à la l-ième coordonnée,*

$$\sum_{j \neq l} \sum_{1 \leq i_j \leq n} h(i_1, \ldots, x, \ldots, i_j, \ldots, i_k) h(i_1, \ldots, y, \ldots, i_j, \ldots, i_k) = n^{k-1} \delta_{xy}$$

Il est étonnamment simple de construire des matrices de Hadamard à k dimensions à partir de simples matrices de Hadamard, de même ordre. En effet, si $H = [h(i_1, i_2)]$ est une matrice de Hadamard d'ordre n, alors $A = [a(i_1, i_2, \ldots, i_k)]$ est une matrice de Hadamard à k dimensions d'ordre n, où

$$a(i_1, i_2, \ldots, i_k) = \prod_{1 \leq u < v \leq k} h(i_u, i_v)$$

Il n'est toutefois pas nécessaire de recourir à ces méthodes pour en obtenir. On a donc une conjecture plus forte que celle de Hadamard.

Problème 8 *Soit $k \geq 4$. Existe-t-il une matrice de Hadamard à k dimensions pour chaque ordre n pair ?*

Enfin le livre de K. J. Horadam contient 90 problèmes de recherche, dont plusieurs peuvent servir, et vont probablement *me* servir, de projet de maîtrise, ou tout simplement, d'occasion d'atteindre un peu de prestige en résolvant une conjecture ouverte depuis plus d'un siècle. Il ouvre également la fenêtre de la recherche en cohomologie, à laquelle est dédiée la seconde partie du livre. On y traite aussi abondamment des applications, dont j'ai peu discuté ici, par choix personnel.

Références

[1] K. J. Horadam. *Hadamard matrices and their applications*, Princeton University Press, 2007.

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 29-32

Marches aléatoires

Maxime Genest
superviseur : Claude Bélisle

Durant l'été 2007, j'eu la chance de travailler sur les chaînes de Markov sous la supervision de Monsieur Claude Bélisle. Il me fait plaisir de partager cette expérience avec vous par l'entremise de ce journal.

Une chaîne de Markov est une suite de variable aléatoire $(V_n)_{n\geq 0}$ à valeur dans un espace d'états E finis ou infinis dénombrable tel que

$\forall\ n \geq 0 \ \ et \ \ \forall\ i_0, i_1, .., i_n, j \in E,$

$$\mathbb{P}\left[V_{n+1} = j \mid V_n = i_n, V_{n-1} = i_{n-1}, ..., V_0 = i_0\right] = \mathbb{P}\left[V_{n+1} = j \mid V_n = i_n\right] \quad (1)$$

à condition que les deux membres de la dernière égalité soient bien définis.

Les chaînes de Markov ont de multiples applications en biologie, économie et bien d'autres domaines. L'étude des chaînes de Markov m'a ensuite mené vers une catégorie bien connue des celles-ci, les marches aléatoires. Lançons nous tout de suite dans le vif du sujet.

Une marhe aléatoire est une chaîne de Markov tel que $E = \mathbb{Z}^d$, $d \in \mathbb{N}$ et

$V_n = \nu_0 + \eta_1 + \eta_2 + ... + \eta_n,$

où $(\eta_n)_{n>0}$ est une suite de variables aléatoires (v.a.) indépendantes et identiquements distribuées (i.i.d) à valeur dans $\mathbb{E}$. ν_0 est également une v.a. sur E et sa distribution de de probabilité est appelée la loi initiale de la marche.

Comme la suite $(\eta_n)_{n>0}$ est i.i.d, alors une marche aléatoire est entièrement définit par la distribution de ν_0 et η_1.

Un aspect intéressant des marches aléatoires est l'étude de la récurrence. Une marche aléatoire est dite récurrente si $\forall i \in \mathbb{Z}^d$,

$$\mathbb{P}[\exists\ T > 0 : V_T = i \mid V_0 = i] = 1 \quad (2)$$

et est dite transitoire sinon.

Remarque : Il suffit de vérifier que l'équation (2) est satisfaite ou non satisfaite pour un seul état i pour conclure sur la récurrence de la marche. La plupart du temps, on prend $i = (0, 0, ..., 0)$ pour vérifier (2).

Un résultat intéressant et bien connu sur la récurrence des marches aléatoires simples et symétriques réside dans le théorème suivant :

Théorème de Pólya (1921)

La marche aléatoire simple et symétrique est :
récurrente si $d = 1$ (R1),
récurrente si $d = 2$ (R2),
et transitoire si $d \geq 3$.

En résumé, si la variable aléatoire η_1 définit une marhce aléatoire simple et symétrique, c'est à dire qu'elle possède une distribution uniforme sur les $2d$ voisins à coordonnées entières de l'origine (exemple : Sur $\mathbb{Z}^2$, on aura η_1 distribuée uniformément sur $\{(-1, 0), (1, 0), (0, -1), (0, 1)\}$), alors un éventuel retour de la marche au point de départ est assuré si $d = 1$ ou $d = 2$, mais incertain si $d \geq 3$. Par exemple, pour $d = 3$, la probabilité d'un retour au point de départ est d'environ 0.340537330....

Ce résultat peut susciter beaucoup de questions. Entre autre, où ce trouve la limite entre la récurrence et le transitoire lorsque l'on parle de marche aléatoire simple et symétrique ?

C'est en fait cette question qui fut l'objet de ma recherche pendant une partie de l'été.

Pour tenter de répondre à cette question, il nous faut quelques outils supplémentaires. Il nous faut d'abord introduire une antité très importante en théorie des probabilités. C'est à dire la fonction caractéristique d'une variable aléatoire.

La fonction caractéristique d'une variable aléatoire X est la fonction ψ de $\mathbb{R}$ vers $\mathbb{C}$ définit comme suit :

$$\psi(u) = \mathbb{E}[e^{iuX}] \tag{3}$$

Les fonctions caractéristiques vérifient plusieurs propriétés dont la plus importante est la suivante :

Il existe une bijection entre la famille de distributions de probabilité sur $\mathbb{R}$ et la famille de fonctions caractéristiques. De plus si ρ désigne une fonction de masse sur d'une variable aléatoire X à valeur dans $\mathbb{R}$ et si $x_1 < x_2$, alors on a la formule de correspondance suivante :

$$\rho((x_1, x_2)) + \frac{1}{2}\rho(\{x_1\}) + \frac{1}{2}\rho(\{x_2\}) = \lim_{T\to\infty} \frac{1}{2\pi} \int_{-T}^{T} e^{-ixu}\psi(u)du \tag{4}$$

où ψ est la fonction caractéristique de la variable aléatoire X.
Note : l'intégrande est définit pas continuité en $t = 0$.

Lorsque X est une variable aléatoire continue sur $\mathbb{R}$, alors la formule de correspondance se réduit à la transformé de Fourier.

Le concept de fonction caractéristique peut s'avérer très utile dans l'étude de la récurrence d'une marche aléatoire en raison du lien tissé par le théorème suivant :

Théorème de récurrence

une marche aléatoire sur $\mathbb{Z}$ est transitoire si et seulement si

$$\int_{-\pi}^{\pi} \Re e \left[\frac{1}{1-\phi(\theta)} \right] d\theta < \infty$$

où $\phi(\theta)$ est la fonction caractéristique de la v.a. η_1

Il est maintenant possible de s'attaquer à la question posée précédemment. La question peut nous mener à l'étude d'une série de modèles de marche aléatoire dont on doit vérifier sur chacun la récurrence. On présentera ici deux modèles qui nous donne des résultats les plus générales possibles.

Modèle A

On pose d'abord $(S_i)_{i\in\mathbb{Z}}$ une suite de sous-ensembles non-vides de $\mathbb{Z}^2$.
On définit ensuite S le sous-ensemble de $\mathbb{Z}^3$ suivant : $S := \{(X,Y,Z) : (X,Y) \in S_i \text{ et } Z = i\}$

Caractérisons maintenant la marche aléatoire :
-Marche aléatoire simple.
-Espace d'états : $\mathbb{Z}^3$
-Définition de la suite de v.a. associée : $(V_n = (X_n, Y_n, Z_n))_{n\geq 0}$ avec

$$V_{n+1} = \begin{cases} V_n + (I_{n+1}, J_{n+1}, K_{n+1}) & \text{si } V_n \in S \\ V_n + (I'_{n+1}, J'_{n+1}, K'_{n+1}) & \text{sinon} \end{cases}$$

où $(I_{n+1}, J_{n+1}, K_{n+1})_{n\geq 0}$ i.i.d uniforme sur $\{(-1,0,0),(1,0,0),(0,-1,0),(0,1,0),(0,0,-1),(0,0,1)\}$

et $(I'_{n+1}, J'_{n+1}, K'_{n+1})_{n\geq 0}$ i.i.d uniforme sur $\{(-1,0,0),(1,0,0),(0,-1,0),(0,1,0)\}$

Autrement dit, on considère une infinité de copies de $\mathbb{Z}^2$ parallèles où il est possible de passer d'un plan à un autre seulement lorsque l'on se retrouve dans l'ensemble de points S.
Note : Ce modèle ne respecte pas la définition de marche aléatoire donnée auparavant. Néanmoins, on parlera quand même de marche aléatoire et de récurrence en prolongeant de façons naturelle la définition

Question : Est-ce que la marche aléatoire associée à ce modèle est récurrente ?

La réponse est partielle. Si

$$\exists\, i \in \mathbb{Z} \text{ tel que } \mid S_i \mid < \infty \tag{5}$$

Alors, il est possible en utilisant les résultats (R1) et (R2) du théorème de Pólya, de montrer que ce modèle définit une marche récurrente.

Par contre, si (5) n'est pas satisfaite. Alors la réponse est restée introuvée. Cependant, Si on considère le modèle A en posant

$$S_i = \{(X, Y) : X = 0 \text{ et } Y \in \mathbb{Z}\} \quad \forall i \in \mathbb{Z} \tag{6}$$

Appelons ce modèle A_Z.

Il est alors possible de ramener l'etude de la récurrence de cette marche à l'étude de la récurrence d'une marche aléatoire sur $\mathbb{Z}$. Cette dernière marche, que l'on peut nommer $(W_n)_{n\geq 0}$, vérifie la définition donnée précédemment d'une marche aléatoire. Il est ensuite possible, à l'aide de méthodes de conditionnement et en utilisant la propriété de Markov, d'identifier la fonction caractéristique de la variable aléatoire η_1 associée à la marche $(W_n)_{n\geq 0}$. En fait, on trouve que cette fonction caractéristique est

$$\psi(u) = 1 - \frac{1}{3}\sqrt{2\sqrt{(2-\cos(u))^2 - 1} + (2-\cos(u))^2 - 1}$$

On peut maintenant étudier la récurrence de la marche $(W_n)_{\geq 0}$ à l'aide du théoreme de récurrence.

On doit vérifier si l'intégrale suivante converge ou diverge :

$$\int_{-\pi}^{\pi} \frac{3}{\sqrt{2\sqrt{(2-\cos(u))^2 - 1} + (2-\cos(u))^2 - 1}} du$$

Il n'est pas trop difficile de montrer que la dernière intégrale converge si et seulement si

$$\int_0^{\pi} \frac{3}{\sqrt{2}\sqrt{u}} du$$

converge, ce qui est le cas.

$$\Longrightarrow \quad \text{Le modèle } \mathrm{A}_Z \text{ définit une marche transitoire.}$$

Conclusion

On vient d'obtenir un exemple de modèle de marche aléatoire tel que (5) n'était pas satisfaite et tel que la marche était transitoire. La symétrie du modèle joue par contre un rôle crûcial dans la résolution. Ce qui laisse entrevoir que cette méthode serait peut-être périeuse pour l'obtention d'un résultat plus général.

Il reste maintenant à éclaircir la question suivante :

Est-ce que

(5) $\Rightarrow$ La marche est transitoire.

À suivre...

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 33-39

Sommes Binomiales

François Guay et Christine Paradis
superviseurs : Frédéric Gourdeau et Javad Mashreghi

Résumé

Soit $(a_n)_{n\geq 0}$ une suite de nombres complexes et soit, pour $n \geq 0$,

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k \qquad \text{et} \qquad c_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_k.$$

Cet article présente certains résultats sur la croissance de la suite (a_n) en fonction de la croissance des suites (b_n) et (c_n). De surcroît, on y expose quelques notions et principes fondamentaux en analyse complexe qui sont nécessaires à la compréhension des démonstrations de ces résultats qui, a priori, semblent éloignés de la théorie portant sur les fonctions complexes.

1 Introduction et présentation des résultats

Tout au long de cet article, nous fixons la notation suivante : soit $(a_n)_{n\geq 0}$ une suite de nombres complexes et soit, pour $n \geq 0$,

$$b_n = \sum_{k=0}^{n} \binom{n}{k} a_k \qquad \text{et} \qquad c_n = \sum_{k=0}^{n} \binom{n}{k} (-1)^{n-k} a_k.$$

Dans un premier temps, le problème concernant la croissance de la suite (a_n) en fonction de la croissance des suites (b_n) et (c_n) a été étudié par I. Chalendar, K. Kellay et T. Ransford. D'ailleurs, dans un article publié en 2000, ils ont présenté le théorème suivant :

Théorème 1 *Soit $(a_n)_{n\geq 0}$ une suite de nombres complexes et soit r un entier non négatif. On suppose que*

$$\sum_{k=0,\ k\ pair}^{n} \binom{n}{k} a_k = O(n^r) \quad \textit{et} \quad \sum_{k=0,\ k\ impair}^{n} \binom{n}{k} a_k = O(n^r) \ \textit{quand}\ n \to \infty.$$

Alors, $a_n = 0$ pour tout $n > r$.

Par la suite, J. Mashreghi et T. Ransford ont travaillé sur un autre aspect de la question et ont tenté d'améliorer le résultat obtenu précédemment. En 2005, ils ont présenté ce théorème :

Théorème 2 *Soit $\beta > 1$. Si $b_n, c_n = O(\beta^n)$, alors $a_n = O(\alpha^n)$, quand $n \to \infty$, où $\alpha = \sqrt{\beta^2 - 1}$, et*

$$\limsup_{n\to\infty} \frac{|a_n|}{\alpha^n} \leq 2\left(\limsup_{n\to\infty} \frac{|b_n|}{\beta^n}\right)^{\frac{1}{2}} \left(\limsup_{n\to\infty} \frac{|c_n|}{\beta^n}\right)^{\frac{1}{2}}.$$

Quant à nous, cet été, nous avons, entre autres, essayé de vérifier si la constante 2 dans cette inégalité est optimale. D'ailleurs, on peut s'assurer que cette constante ne peut pas être inférieure à $\frac{2}{\sqrt{3}}$ en considérant la suite $a_n = (i\sqrt{3})^n - (-i\sqrt{3})^n$ avec $\alpha = \sqrt{3}$.

De plus, on s'est attardé à une nouvelle question en posant les hypothèses suivantes.

Soit $(\alpha_n)_{n\geq 0}$ et $(\beta_n)_{n\geq 0}$ deux suites de nombres complexes et soit r un entier non négatif.

Supposons que

$$\begin{aligned} b_n &= \sum_{k=0}^{n} \binom{n}{k} \alpha_k \beta_{n-k} = O(n^r) \quad \text{quand } n \to \infty, \\ c_n &= \sum_{k=0}^{n} \binom{n}{k} (-1)^k \alpha_k \beta_{n-k} = O(n^r) \quad \text{quand } n \to \infty. \end{aligned}$$

Notre tâche était de tirer des résultats à partir de ces nouvelles hypothèses. On remarque qu'en posant la suite $\beta_n \equiv 1$ pour tout n, on retrouve les hypothèses du théorème 1. On se trouve donc devant une généralisation du théorème 1.

Par ailleurs, les démonstrations des deux théorèmes présentés ci-haut ne seront pas présentées dans ce document-ci. Cependant, il est possible d'en connaître les détails en consultant [1] et [2]. Dans les sections qui suivent, il vous sera possible de survoler en quelques pages les résultats avec lesquels nous avons dû nous familiariser pour arriver à comprendre ces deux démonstrations.

2 Notions de base en analyse complexe

2.1 Définitions

Définition 1 *Une fonction $f(x,y) = u(x,y) + iv(x,y)$ est dite $\mathbb{C}$-différentiable en $z_0 = x_0 + iy_0$ si et seulement si f est différentiable au sens réel en z_0 et que, de plus, elle vérifie les équations de Cauchy-Riemann en ce point. On peut écrire ces équations sous cette forme :*

$$\frac{\partial u}{\partial x}(x_0,y_0) = \frac{\partial v}{\partial y}(x_0,y_0) \qquad et \qquad \frac{\partial u}{\partial y}(x_0,y_0) = -\frac{\partial v}{\partial x}(x_0,y_0)$$

Ces équations impliquent que les fonctions $u(x,y)$ et $v(x,y)$ sont harmoniques.

Soit $f : \mathcal{O} \to \mathbb{C}$ une fonction à variable complexe, où $\mathcal{O}$ est un ouvert de $\mathbb{C}$.

Définition 2 *f est holomorphe sur $\mathcal{O}$ si elle est $\mathbb{C}$-différentiable en tout point de $\mathcal{O}$.*

Définition 3 *f est analytique sur $\mathcal{O}$ si elle est développable en série entière convergente au voisinage de chaque point de $\mathcal{O}$.*

Une fonction f est holomorphe sur un ouvert $\mathcal{O}$ si et seulement si f est analytique sur $\mathcal{O}$.

Définition 4 *Une fonction entière est une fonction holomorphe sur tout le plan complexe.*

2.2 Quelques propriétés des fonctions analytiques

Théorème 3 *Si une fonction f est analytique sur un domaine $\mathcal{D}$ simplement connexe, alors*

$$\int_{\mathcal{C}} f(z)\, dz = 0$$

pour toute courbe $\mathcal{C}$ fermée dans $\mathcal{D}$.

Théorème 4 *Soit f une fonction analytique à l'intérieur et sur une courbe simple fermée $\mathcal{C}$, orientée positivement. Si z est un point à l'intérieur de $\mathcal{C}$, alors*

$$f^{(n)}(z) = \frac{n!}{2\pi i} \int_{\mathcal{C}} \frac{f(w)}{(w-z)^{n+1}}\, dw \qquad \forall n \in \{0,1,2,...\}$$

3 Principe du maximum

3.1 Fonctions harmoniques

Définition 5 *Une fonction à valeurs réelles $u(x,y)$, deux fois continûment dérivable, définie sur un ensemble ouvert $\mathcal{O} \subseteq \mathbb{R}^2$, est dite harmonique si et seulement si*

$$\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} = 0$$

dans $\mathcal{O}$.
De plus, si $u(z)$ est harmonique sur $\mathcal{O}$, $z_0 \in \mathcal{O}$ et $r < d(z_0, \partial\mathcal{O})$, alors

$$u(z_0) = \frac{1}{2\pi} \int_0^{2\pi} u(z_0 + re^{i\theta})\, d\theta.$$

Théorème 5 *Soit $\mathcal{O}$ un ensemble ouvert et borné. Soit $u(z)$ une fonction harmonique dans $\mathcal{O}$ et continue sur $\overline{\mathcal{O}}$. Si $u(z) \leq M$ sur $\partial\mathcal{O}$, alors*
$u(z) \leq M$ aussi sur $\mathcal{O}$.

3.2 Fonctions sous-harmoniques

Définition 6 *Soit $\mathcal{D}$ un ouvert de $\mathbb{C}$. Une fonction $u : \mathcal{D} \to [-\infty, \infty)$ est dite semi-continue supérieurement si l'ensemble $\{z \in \mathcal{D} : u(z) < c\}$ est ouvert $\forall c \in \mathbb{R}$. De plus, u est semi-continue supérieurement si et seulement si*

$$\limsup_{z \to z_0,\ z \neq z_0} u(z) \leq u(z_0) \qquad\qquad \forall z_0 \in \mathcal{D}.$$

Définition 7 *La fonction $u : \mathcal{D} \to [-\infty, \infty)$ est sous-harmonique sur $\mathcal{D}$ si elle est semi-continue supérieurement et si, pour tout $z \in \mathcal{D}$, il existe $r_z > 0$, avec $\{w : |w - z| \leq r_z\} \subset \mathcal{D}$, tel que*

$$u(z_0) \leq \frac{1}{2\pi} \int_0^{2\pi} u(z_0 + re^{i\theta})\, d\theta$$

pour $r < r_z$.

Théorème 6 *Soit $\mathcal{D}$ un domaine borné et soit $u(z)$ une fonction sous-harmonique sur $\mathcal{D}$ et semi-continue supérieurement sur $\overline{\mathcal{D}}$. Alors, il existe $z_0 \in \partial\mathcal{D}$ tel que $u(z) \leq u(z_0)$ pour tout $z \in \mathcal{D}$.*

Théorème 7 (Phragmén-Lindelöf) *Soit $u(z)$ une fonction sous-harmonique sur un secteur angulaire $\mathcal{S}$, issu de l'origine et d'angle 2γ, où $0 < \gamma \leq \frac{\pi}{2}$. Supposons, $\forall \zeta \in \partial\mathcal{S}$,*

$$\limsup_{z \in \mathcal{S},\ z \to \zeta} u(z) \leq M.$$

S'il existe $\alpha < \frac{\pi}{2\gamma}$ et $C > 0$ tels que $u(z) \leq C|z|^\alpha$, alors $u(z) \leq M$ dans $\mathcal{S}$.

4 Analyse asymptotique

4.1 Notations asymptotiques

Étant donné que les théorémes étudiés énoncent des résultats sur l'ordre de croissance de la suite $(a_n)_{n\geq 0}$, il s'avère pertinent de définir formellement quelques notations de Landau.

Définition 8 (Notation O) *Si $f(n) = O\{g(n)\}$, quand $n \to \infty$, alors $\left|\frac{f(n)}{g(n)}\right|$ est borné pour tous les n plus grands qu'un certain N. À l'aide de quantificateurs universels, on exprime cette définition comme suit :*
$f(n) = O\{g(n)\}\,(n \to \infty) \Leftrightarrow \exists M > 0, \exists\, N, \forall n > N, |f(n)| \leq M|g(n)|.$

Définition 9 (Notation o) *$f(n) = o\{g(n)\}$ signifie que $\left|\frac{f(n)}{g(n)}\right| \to 0$ quand $n \to \infty$. À l'aide de quantificateurs universels, on exprime cette définition comme suit :*
$f(n) = o\{g(n)\}\,(n \to \infty) \Leftrightarrow \forall M > 0, \exists\, N, \forall n > N, |f(n)| < M|g(n)|.$

4.2 Méthode de Laplace

En parcourant les lignes de la démonstration du théorème 2, vous rencontrerez cette égalité :

$$\frac{1}{2\pi}\int_0^{2\pi} e^{\alpha r|\sin\theta|}\,d\theta = \left(\sqrt{\frac{2}{\pi}} + o(1)\right)\frac{e^{\alpha r}}{\sqrt{\alpha r}} \quad \text{quand } r \to \infty$$

et alors, vous vous demanderez probablement comment il est possible d'arriver à un tel résultat. En étudiant la méthode de Laplace, vous trouverez la solution à ce problème.

Tout d'abord, on a que

$$\frac{1}{2\pi}\int_0^{2\pi} e^{\alpha r|\sin\theta|}\,d\theta = \frac{1}{\pi}\int_0^{\pi} e^{\alpha r\sin\theta}\,d\theta.$$

L'idée générale de la méthode de Laplace est la suivante : puisque sur l'intervalle [0,π], sin θ possède un maximum global en $\frac{\pi}{2}$, seul le voisinage de $\frac{\pi}{2}$ contribue à l'intégrale lorsque $r \to \infty$.

Ainsi, on pose $I(r) = \frac{1}{\pi}\int_0^{\pi} e^{\alpha r\sin\theta}\,d\theta$. Puis, on approxime $I(r)$ par
$I(r,\varepsilon) = \frac{1}{\pi}\int_{\frac{\pi}{2}-\varepsilon}^{\frac{\pi}{2}+\varepsilon} e^{\alpha r\sin\theta}\,d\theta$ où $0 < \varepsilon < \frac{\pi}{2}$ est arbitraire.

Par la suite, on remplace la fonction sin θ par les premiers termes de son développement en série de Taylor autour de $\frac{\pi}{2}$. On obtient

$$I(r) \sim \frac{1}{\pi}\int_{\frac{\pi}{2}-\varepsilon}^{\frac{\pi}{2}+\varepsilon} e^{\alpha r(1-\frac{1}{2}(\theta-\frac{\pi}{2})^2)}\,d\theta.$$

Ensuite, on peut évaluer cette intégrale entre $-\infty$ et ∞, introduisant ainsi que des erreurs négligeables.

$$\begin{aligned} I(r) &\sim \frac{1}{\pi}\int_{-\infty}^{\infty} e^{\alpha r(1-\frac{1}{2}(\theta-\frac{\pi}{2})^2)}\, d\theta \\ &\sim \frac{e^{\alpha r}}{\pi}\int_{-\infty}^{\infty} e^{-\frac{\alpha r}{2}(\theta-\frac{\pi}{2})^2}\, d\theta \end{aligned}$$

Enfin, en posant $s = \sqrt{\frac{\alpha r}{2}}(\theta - \frac{\pi}{2})$, on obtient

$$\begin{aligned} I(r) &\sim \frac{\sqrt{2}}{\pi}\frac{e^{\alpha r}}{\sqrt{\alpha r}}\int_{-\infty}^{\infty} e^{-s^2}\, ds \\ &\sim \sqrt{\frac{2}{\pi}}\frac{e^{\alpha r}}{\sqrt{\alpha r}} \end{aligned}$$

On obtient ainsi le résultat désiré.

5 Fonctions entières de type exponentiel

Voici trois manières différentes, mais équivalentes de définir une fonction de type exponentiel :

Définition 10 *Une fonction entière f(z) est dite de type exponentiel s'il existe des constantes $\alpha > 0$ et $K > 0$ pour lesquelles on a la relation suivante :*

$$|f(z)| \leq Ke^{\alpha|z|}.$$

Définition 11 *Une fonction entière f(z) est dite de type exponentiel τ si*

$$\tau = \limsup_{|z|\to\infty} \frac{\log|f(z)|}{|z|} < \infty.$$

Définition 12 *Une fonction entière $f(z) = \sum_{n=0}^{\infty} a_n z^n$ est dite de type exponentiel τ si*

$$\tau = \frac{1}{e}\limsup_{n\to\infty} n\sqrt[n]{|a_n|} < \infty.$$

Définition 13 *Une fonction entière f(z) est dite de type exponentiel minimal si $\tau = 0$.*

Conclusion

Somme toute, ce projet de recherche nous a permis d'approfondir notre compréhension de plusieurs résultats fondamentaux en analyse, d'en apprendre davantage sur des concepts et notions plus complexes et même d'aborder des sujets traités seulement en fin de baccalauréat ou à la maîtrise. Ce fut une expérience très enrichissante. Enfin, nous tenons à remercier Frédéric Gourdeau et Javad Mashreghi pour leur soutien tout au long de l'été.

Références

[1] J. MASHREGHI, T. RANSFORD, *Binomial sums and functions of exponential type*, London Mathematical Society. **37** (2005) 15-24.

[2] I. CHALENDAR, K. KELLAY et T. RANSFORD, *Binomial sums, moments and invarant subspaces*, Israël J. Math. **115** (2000) 303-320.

[3] J. BAK, D. J. NEWMAN, *Complex analysis*, Springer-Verlag, New York, deuxième édition, 1997.

[4] J. MASHREGHI, *Representation theorems in Hardy Spaces*, chapitre 4, pré-impression.

[5] J.W. BROWN, R.V. CHURCHILL *Complex variables and applications*, McGraw-Hill, New York, sixième édition, 1996.

[6] A.I. MARKUSHEVICH *Entire functions*, American Elsevier, New York, 1966.

[7] A.I. MARKUSHEVICH *Theory of functions of a complex variable volume II*, Prentice-Hall, Englewood Cliffs, N.J., 1965.

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 41-44

Équations diophantiennes

Benoît Pouliot, Alexandre St-Onge et Malik Younsi

Résumé

Lors de notre première bourse de recherche à l'été 2006, nous nous sommes intéressés à quelques problèmes que nous avons résolus en groupe. Dans cet article, nous vous présentons celui qui nous semble le plus intéressant. Nous proposons donc une étude de l'équation diophantienne suivante :

$$x^k + y^{k+1} = z^{k+2}$$

1 Introduction

L'étude des équations diophantiennes est un chapitre important dans la théorie des nombres. La forme générale d'une telle équation est,

$$x^a + y^b = z^c \qquad \text{où } x, y, z, a, b, c \in \mathbb{N}. \tag{1}$$

À l'exemple de l'équation pythagoricienne, $x^2 + y^2 = z^2$, qui possède une infinité de solutions, nous voulons savoir si l'équation spécifique de départ

$$x^k + y^{k+1} = z^{k+2}$$

possède ou non une infinité de solutions. Nous allons donc répondre à cette question.

2 Résolution du problème

Voici le résultat obtenu,

Théorème 1
L'équation diophantienne suivante,

$$x^k + y^{k+1} = z^{k+2} \tag{2}$$

possède une infinité de solutions $\forall k \in \mathbb{N}$.

Le but de cet article est d'exposer notre raisonnement. Il se peut qu'il existe des théorèmes pour lesquels notre résultat est une simple application. Notre démonstration est cependant constructive et elle montre bien le cheminement que nous avons fait.

Démonstration. Pour commencer, nous avons séparé le problème en deux en étudiant séparément les cas où k est impair et pair.

-k impair

À la suite de quelques calculs et exemples, ce cas s'est avéré plus simple que prévu. En effet, nous allons montrer que l'équation (2) avec k impair possède toujours une solution de la forme,

$$\begin{aligned}(n^A(n+1)^B)^k + (n^C(n+1)^D)^{k+1} &= (n^E(n+1)^F)^{k+2} \\ A, B, C, D, E, F, n &\in \mathbb{N}\end{aligned} \tag{3}$$

On pose $kB = D(k+1)$ et $kA-1 = C(k+1)$, de façon à avoir :

$$\begin{aligned}n^{kA}(n+1)^{kB} + n^{kA-1}(n+1)^{kB} &= n^{E(k+2)}(n+1)^{F(k+2)} \\ \iff n^{kA-1}(n+1)^{kB}(n+1) &= n^{E(k+2)}(n+1)^{F(k+2)} \\ \iff n^{kA-1}(n+1)^{kB+1} &= n^{E(k+2)}(n+1)^{F(k+2)}\end{aligned}$$

On a donc les équations :

$$\begin{aligned}kA-1 &= E(k+2) \\ kB+1 &= F(k+2) \\ kB &= D(k+1) \\ kA-1 &= C(k+1)\end{aligned}$$

En résolvant le système de congruences associé, on obtient :

$$\begin{aligned}A &= \tfrac{1}{2}(k^2+2k-1) \\ B &= \tfrac{1}{2}((k+1)^2) \\ C &= \tfrac{1}{2}(k-1)(k+2) \\ D &= \tfrac{1}{2}k(k+1) \\ E &= \tfrac{1}{2}(k-1)(k+1) \\ F &= \tfrac{1}{2}(k^2+1)\end{aligned}$$

Il est donc possible de déterminer A,B,C,D,E et F dans (3), et ce $\forall k$ impair. De plus, cette méthode génère une infinité de solutions puisqu'elle est valable $\forall n \in \mathbb{N}$. Ceci complète la démonstration pour le cas impair.

Remarque

Il est intéressant de constater que la méthode précédente fonctionne également pour des valeurs négatives impaires de k. On peut donc trouver des solutions à l'équation suivante :

$$\frac{1}{x^t} + \frac{1}{y^{t-1}} \;=\; \frac{1}{z^{t-2}} \qquad x, y, z, t \in \mathbb{N} \qquad (t \geq 3 \;,\; t \; impair)$$

-k pair

Ce deuxième cas a été, pour nous, plus compliqué. Nous n'avons pas trouvé de forme générale comme pour le cas impair. Nous nous sommes donc ramenés à une autre forme d'équation diophantienne pour arriver à notre but. En effet, nous avons considéré l'équation diophantienne suivante :

$$a^k + b^{k+1} \;=\; c^k \qquad k \in \mathbb{N} \tag{4}$$

où l'on prend $a,\ b,\ c \;\in \mathbb{N}$ et $c \;=\; a + b$. La remarque la plus importante est qu'une telle équation possède toujours au moins une solution. Il suffit de prendre,

$$a \;=\; 2^k - 1 \;=\; b \quad \text{et} \quad c \;=\; 2(2^k - 1)$$

pour s'en convaincre.

C'est avec une équation du type (4) que nous sommes parvenus à résoudre le cas pair. Il est de plus intéressant de noter que la démonstration que nous allons faire est aussi valide pour le cas impair. Donc, il n'est pas nécessaire de séparer ce problème en deux, cependant, lors de la résolution, cela nous semblait approprié. Nous allons maintenant montrer qu'à partir de toute solution de (4) nous pouvons trouver une solution de (2).

Soit a, b, c une solution de (4), alors on a :

$$\begin{aligned}
a^k + b^{k+1} \;&=\; c^k \\
\iff (a+b)^{k(k+1)}(a^k + b^{k+1}) \;&=\; (a+b)^{k(k+1)}c^k \\
\iff \left(a(a+b)^{k+1}\right)^k + \left(b(a+b)^k\right)^{k+1} \;&=\; (a+b)^{k(k+1)+k} \\
\iff \left(a(a+b)^{k+1}\right)^k + \left(b(a+b)^k\right)^{k+1} \;&=\; \left((a+b)^k\right)^{k+2} \\
\iff x^k + y^{k+1} \;&=\; z^{k+2}
\end{aligned}$$

où $x \;=\; a(a+b)^{k+1}$, $y \;=\; b(a+b)^k$ *et* $z \;=\; (a+b)^k$. Ce qui montre l'existence de solutions.

Il suffit maintenant de montrer que l'équation (2) possède une infinité de solutions pour le cas où k est pair. Soit α, β et γ tels que

$$\alpha^k + \beta^{k+1} \;=\; \gamma^{k+2}.$$

On multiplie de chaque côté de l'équation par $r^{k(k+1)(k+2)}$ pour un certain r $\in \mathbb{N}$. On obtient :

$$(\alpha r^{(k+1)(k+2)})^k + (\beta r^{k(k+2)})^{k+1} \;=\; (\gamma r^{k(k+1)})^{k+2}.$$

Ceci est une nouvelle solution de l'équation diophantienne et ainsi, on a une infinité de solutions. La démonstration du théorème est complété.

□

3 Conclusion

Même si ce résultat n'est pas des plus importants, il reste intéressant du point de vue de la résolution de problème. Pour nous, ce problème est une belle application de la théorie des nombres. Nous avons cherché en équipe pendant une ou deux semaines afin d'obtenir la solution complète. Bien que l'on ne génère pas tous les cas, notre démarche permet de construire plusieurs solutions. C'est donc un plaisir d'avoir présenté notre méthode de pensée pour ce problème.

Journal du groupe de recherche des étudiant(e)s
en mathématiques de l'université Laval
Volume 1, septembre 2007, 45-46

Le comportement asymptotique d'un lancer de pièce de monnaie et sa généralisation

Jean-Philippe Labbé

Résumé

Étant donné deux entiers positifs k et n, désignons par $F(k,n)$ la probabilité d'obtenir k piles d'affilée en lançant n fois une pièce de monnaie équilibrée. Je présente ici l'étude du comportement asymptotique de la fonction $F(k,n)$ lorsque $n \to \infty$ ainsi que l'étude de la valeur médiane asymptotique de $F(k,n)$ lorsque $n \to \infty$. En modifiant les résultats précédents, on obtient aisément les résultats pour le lancer d'un dé équilibré à ℓ faces.

Introduction

Ce problème m'a été présenté par Nicolas Doyon durant l'été 2007. Il est présenter à l'aide du concept très familier qu'est le lancer d'une pièce de monnaie. Qu'advient-il des suites de piles consécutives lors d'une succession de lancer ? Par exemple, sommes-nous assurer d'avoir 5 piles d'affiler si nous lançons 200 fois la pièce de monnaie ? Avec quelle probabilité ? L'étude de la fonction F permet de répondre à ces questions et plus encore.

Lancer d'une pièce de monnaie équilibrée

Énonçons d'abord les problèmes initiaux. Étant donné deux entiers positifs k et n, désignons par $F(k,n)$ la probabilité d'obtenir k piles d'affilée en lançant n fois une pièce de monnaie équilibrée. Ainsi $F(k,n) = 0$ si $k > n$ et $F(k,n) = 1$ si $k \leq 0$.

Problème 1. Pour k fixe, quel est le comportement asymptotique de $F(k,n)$ lorsque $n \to \infty$?

Problème 2. Définissons la fonction $H(n)$ implicitement par les deux inégalités suivantes :

1. $F(H(n),n) \geq 1/2$;
2. $F(H(n)+1,n) < 1/2$.

Quel est le comportement asymptotique de $H(n)$ lorsque $n \to \infty$?

Pour répondre aux questions, j'ai fait appel à des méthodes de dénombrements, des résultats d'analyse et d'analyse complexe. Voici les résultats obtenus.

Théorème 1 *La fonction F s'écrit de façon explicite sous la forme*

$$F(k,n) = 1 - C(k)\left(1 - \frac{1}{2^{k+1}}\right)^n \qquad (n \to \infty), \tag{1}$$

où $C(k) := (2^k - 1)2^{k^2}/(2^{k+1} - 1)^k$.

Théorème 2 *La fonction $H(n)$ possède la représentation explicite*

$$H(n) = \frac{\log\left(\frac{2n}{\log 2} + 1 + o(1)\right)}{\log 2} - 2 \qquad (n \to \infty). \tag{2}$$

La fonction H détermine la valeur médiane de F. Pour un n fixe, elle donne la valeur maximale de k pour laquelle $F(k,n) \geq 1/2$. Par exemple, si $n = 1000$ on obtient que $H(n) = 9.49505057...$ et donc $F(9,1000) \geq 1/2$ mais $F(10,1000) < 1/2$.

Lancer d'un dé équilibré à ℓ faces

Il est possible, sans trop de difficultés, de généraliser la fonction F pour le lancer d'un dé à $\ell \geq 2$ faces. Ainsi, si ℓ est un entier ≥ 2, on obtient

Théorème 3 *La fonction F_ℓ s'écrit de façon explicite sous la forme*

$$F_\ell(k,n) = 1 - C(k,\ell)\left(1 - \frac{1}{\ell^{k+1}}\right)^n \qquad (n \to \infty), \tag{3}$$

où $C(k,\ell) := (\ell^k - 1)\ell^{k^2}/(\ell^{k+1} - 1)^k$.

et

Théorème 4 *La fonction $H_\ell(n)$ possède la représentation explicite*

$$H_\ell(n) = \frac{\log\left(\frac{2n}{\log 2} + 1 + o(1)\right) - \log 2}{\log \ell} - 1 \qquad (n \to \infty). \tag{4}$$

Conclusion

L'étude de cette fonction de probabilité n'a pas été une tâche facile ; plusieurs nuits de sommeils ont été troublées par ce problème, j'ai dû améliorer mes démonstrations et rédiger l'article de façon plus claire. Je dois remercier Quentin Rajon qui m'a fourni un lemme devenant la pierre angulaire de la démonstration du premier théorème. La prochaine étape sera de lire la demi-douzaine d'articles qui concernent plus particulièrement le lancer d'une pièce de monnaie afin d'éprouver la véracité des résultats.

Remerciements. Je dois dire merci à Jean-Marie De Koninck et Nicolas Doyon pour avoir vérifié mon article à plusieurs reprises et pour leurs remarquent constructives afin d'améliorer sa qualité.