

**2004**  
**IMAGES**  
**DES MATHÉMATIQUES**

Photographie de couverture :

**Création par le compas**

**Barthélemy l'Anglais**

*Livre des propriétés des choses,*

Franciscain né vers 1190 en Angleterre, mort en 1250 au couvent des frères mineurs de Magdebourg, Barthélemy l'Anglais est l'auteur d'une compilation encyclopédique en 19 livres où sont réunies des notions scientifiques tirées des auteurs sacrés et profanes. Le succès de ce *Liber de proprietatis rerum* est attesté par de nombreux manuscrits, plusieurs éditions incunables et des traductions dans toute l'Europe occidentale. La version française a été rédigée à la demande de Charles V par son chapelain Jean Corbechon, maître en théologie. Il en existe de nombreuses copies très luxueuses, dont celle-ci, du XV<sup>e</sup> siècle, qui présente le Créateur muni d'un compas. [Cette copie manuscrite de la traduction française par Jean Corbechon du *Liber de proprietatibus rerum* de Barthélemy l'Anglais, à la riche iconographie, présente le Créateur muni d'un compas.]

© Bibliothèque Sainte-Geneviève, Paris

**Images des mathématiques 2004**

**Directeur de la publication : Michel Lannoo, directeur du département des sciences physiques et mathématiques du CNRS**

**Rédacteurs en chef : Etienne Ghys, Jacques Istas**

**Réalisation-coordination : Frédérique Laubenheimer, communication du département des sciences physiques et mathématiques du CNRS 3, rue Michel-Ange 75794 Paris cedex 16**

**Fabrication : Louis-Jean n° 155**

**ISSN 0994-723 X. Dépôt légal : 269928T. Février 2004**

## Éditorial

Voici un nouveau numéro des « Images des mathématiques », après une longue interruption. A cette occasion, le Département des sciences physiques et mathématiques fait un important effort de diffusion : ce numéro est envoyé aux membres permanents des laboratoires de mathématiques, de physique théorique et d'informatique. Grâce à la bonne volonté de l'Union des professeurs de spéciale, que nous tenons à remercier, ce numéro parviendra aussi aux professeurs de mathématiques des classes préparatoires. Remercions également les sociétés savantes, Société mathématique de France et Société de mathématiques appliquées et industrielles, qui vont aider le CNRS à assurer la meilleure diffusion possible en dehors de ses frontières. Par ailleurs, ce numéro est téléchargeable en .pdf sur le site web du département SPM :

<http://www.spm.cnrs-dir.fr/actions/publications/IdM.htm>

Nous espérons que cet effort de diffusion permettra à cette publication de remplir son rôle : rassembler des articles qui donnent une idée à la fois précise et attrayante de mathématiques en train de se faire à des lecteurs mathématiciens, mais non spécialistes du sujet traité. Nous savons combien cet exercice est difficile et les auteurs s'y sont soumis avec brio, stimulés par l'enthousiasme et le talent d'Étienne Ghys et de Jacques Istas, qui ont assumé tout le travail éditorial de ce numéro. Qu'ils soient ici remerciés.

Ce numéro comprend 18 articles classés, suivant les traditions du milieu, selon l'ordre alphabétique des auteurs. Parmi ceux-ci, remarquons l'article écrit par Laurent Lafforgue, qui a été récompensé en août 2002, au Congrès international des mathématiciens, par une médaille Fields. Son article explique l'origine historique de sa problématique et le profond travail d'unification qu'il a réalisé.

Tous les articles, à des degrés divers, témoignent de cet enracinement historique, de l'unité profonde des mathématiques et de leur ouverture vers les autres champs disciplinaires (dans le désordre : physique, mécanique céleste, économie, mécanique des fluides, chimie, génomique). Regrettons un peu l'absence d'articles illustrant les liens entre mathématiques et informatique. Cette lacune sera comblée, soyons-en sûrs, dans le prochain numéro. Cette ouverture est aussi institutionnelle (des articles ont été écrits par des collègues qui travaillent dans des structures hors des frontières du CNRS).

Unité et ouverture des mathématiques sont les axes stratégiques de la politique scientifique menée par le CNRS en mathématiques. Ce numéro des « Images des mathématiques » est ainsi une illustration de cette politique.

Le département des Sciences physiques  
et mathématiques du CNRS

# L'analyse multifractale des signaux

***L'analyse multifractale, née dans les années 1980 pour expliquer les observations effectuées sur des signaux de turbulence, a fourni de nouveaux outils pour l'analyse et la modélisation de signaux issus de multiples domaines scientifiques. En mathématiques, elle a servi de cadre unificateur pour reconsidérer de nombreuses fonctions introduites au cours des XIX<sup>e</sup> et XX<sup>e</sup> siècles. De nouvelles synergies sont ainsi apparues entre mathématiciens, physiciens et analystes du signal.***

Au milieu des années 1980, les premiers enregistrements très précis de la vitesse d'un écoulement turbulent tels que ceux obtenus dans la soufflerie de Modane (travaux de Gagne, Hopfinger et leurs collaborateurs) ont confirmé la très grande complexité de ces données expérimentales. Les mathématiciens ont l'habitude de considérer des fonctions partout irrégulières ; c'est le cas des fonctions de Weierstrass

$$W_{a,b}(x) = \sum_{n=1}^{\infty} a^n \sin(b^n x)$$

qui sont continues, mais nulle part dérivables si  $0 < a < 1 < ab$ . Il en est de même pour le mouvement brownien. De telles fonctions présentent cependant une certaine forme de régularité : leur irrégularité est en fait partout la même. La théorie de la turbulence homogène et isotrope développée par Kolmogorov en 1941 se situe dans un tel contexte. Toutefois, les expériences récentes révèlent des déviations systématiques par rapport aux prédictions de cette théorie. Les signaux de vitesse turbulente semblent très irréguliers dans certaines régions et beaucoup moins dans d'autres, sans que l'on puisse clairement assigner de frontières à ces régions : au sein d'une zone plutôt régulière on voit des zones d'irrégularité et réciproquement, ce mélange apparaissant à toutes les échelles. Cette complexité « multi-échelle » fait incontestablement penser aux fractals. L'analyse multifractale est apparue en physique pour comprendre et analyser des fonctions aussi complexes et pour introduire de nouveaux paramètres quantitatifs permettant leur classification. En fait, c'est dans les différents modèles de cas-

cade d'énergie proposés par Mandelbrot en turbulence pleinement développée que l'on trouve les prémices de l'analyse multifractale, formalisée en 1985 par Parisi et Frisch dans leur étude des données expérimentales. Parallèlement, Kadanoff et ses collaborateurs à l'université de Chicago ont jeté les bases de cette approche dans le cadre des mesures invariantes de systèmes dynamiques. Une fois les outils conceptuels et numériques mis en place, cette analyse s'est révélée pertinente dans d'autres domaines des sciences fondamentales et appliquées ; c'est le cas pour les diverses manifestations de la turbulence en hydrodynamique, chimie, optique ; mais il existe bien d'autres domaines où l'on observe des structurations dynamiques spatiales, voir spatio-temporelles complexes, très irrégulières relevant des concepts de fractals, ou de multifractals, en physique, géophysique, astrophysique, météorologie, chimie, ou encore biologie, écologie, économie, analyse et synthèse d'image, télécommunications... Parallèlement à l'énergie déployée pour mettre en application cette nouvelle approche, les mathématiciens, eux, construisaient et analysaient de nombreux modèles de fonctions multifractales et, surtout, étudiaient la validité des méthodes numériques mises en œuvre pour caractériser les paramètres qui leur sont associés. Nous exposerons ces méthodes, nommées « formalisme multifractal », et nous donnerons un aperçu des résultats mathématiques que l'on peut obtenir. Nous illustrerons notre propos de quelques applications concernant l'analyse des séquences d'ADN, de signaux de vitesse turbulents, de séries financières et d'images satellite de la structure des nuages.

## QU'EST-CE QUE L'ANALYSE MULTIFRACTALE ?

L'analyse multifractale a pour but l'étude de fonctions dont la régularité ponctuelle peut varier d'un point à un autre. Les premiers outils pour mesurer la régularité sont familiers à tous : continuité, dérivabilité en un point. L'exposant de Hölder introduit un continuum entre ces notions et permet de repérer précisément la régularité grâce à un paramètre réel positif : une fonction  $f$  est  $C^\alpha(x_0)$  s'il existe un polynôme  $P$  de degré au plus  $[\alpha]$  tel que

$$|f(x) - P(x - x_0)| \leq C|x - x_0|^\alpha.$$

L'exposant de Hölder de  $f$  en  $x_0$  est alors

$$H_f(x_0) = \sup\{\alpha : f \text{ est } C^\alpha(x_0)\}.$$

On a vu que l'on s'attend à ce que les ensembles « isohölder »

$$A_h = \{x : H_f(x) = h\}$$

soient des fractals. Si tel est le cas, le paramètre naturel à déterminer est leur dimension de Hausdorff (encadré 1). Finalement, on cherchera donc à calculer la fonction

$$D(h) = \dim(A_h)$$

appelée *spectre de singularités* de  $f$ . Réaliser l'analyse multifractale d'une fonction  $f$ , c'est déterminer son spectre de singularités. Avant de décrire comment calculer numériquement le spectre de signaux expérimentaux, mentionnons quelques fonctions mathématiques multifractales.

## QUELQUES FONCTIONS MULTIFRACTALES

Bien sûr, la notion de fonction multifractale, introduite en physique au milieu des années 1980, n'avait pas pu être utilisée auparavant par les mathématiciens. Mais, comme par anticipation, de nombreuses fonctions – qui se sont ensuite révélées être multifractales – ont été considérées depuis le début du XIX<sup>e</sup> siècle. En général, il s'agissait d'exemples (ou de contre-exemples) ayant des propriétés particulières.

Ainsi, dès que Bolzano et Cauchy eurent, indépendamment, donné la définition mathématique précise d'une fonction continue, la question de l'existence de fonctions continues nulle part dérivables s'est naturellement posée. Le premier exemple d'une telle fonction a été construit par Bolzano lui-même en 1830 ; c'était une fonction en dents de scie, auxquelles on superpose des dents de scie de plus en plus petites... Il s'agit probablement de la première fonction mathématique multifractale. Malheureusement pour Bolzano (mais, nous allons le voir, heureusement pour nous !), cet exemple est resté longtemps ignoré et Riemann mentionnait encore ce problème en proposant comme candidat possible la série trigonométrique

$$\sum_{n=1}^{\infty} \frac{\sin(\pi n^2 x)}{n^2}.$$

On sait maintenant que cette fonction est dérivable en certains rationnels ; en revanche, c'est un très bel exemple de fonction multifractale ; son spectre est la réunion du segment  $D(h) = 4h - 2$  (pour  $h \in \left[\frac{1}{2}, \frac{3}{4}\right]$ ) et du point  $(h, d) = \left(\frac{3}{2}, 0\right)$ .

### Encadré 1

## DIMENSION DE HAUSDORFF

La notion de dimension de Hausdorff étend à des ensembles fractals (dont la dimension pourra être non entière), la notion naturelle de dimension pour les courbes et surfaces régulières. Soit  $A$  un sous-ensemble borné de  $\mathbb{R}^d$ . Une famille  $R = \{B_i\}_{i \in \mathbb{N}}$  d'ensembles  $B_i \subset \mathbb{R}^d$  est un  $\varepsilon$ -recouvrement de  $A$  si  $A \subset \bigcup B_i$  et  $\forall i, \text{diam}(B_i) \leq \varepsilon$ .

On note alors  $M_\varepsilon^\delta = \inf_{R=\{B_i\}} \sum (\text{diam}(B_i))^\delta$ , où l'inf est pris sur tous les  $\varepsilon$ -recouvrements.

La dimension de Hausdorff de  $A$  est alors

$$\dim(A) = \sup\{\delta : \lim_{\varepsilon \rightarrow 0} M_\varepsilon^\delta = +\infty\}.$$

On vérifie aisément que, suivant cette définition, la dimension d'une courbe régulière est 1, d'une surface régulière est 2, mais on peut ainsi obtenir des dimensions non entières. Ainsi l'ensemble triadique de Cantor composé des nombres réels

s'écrivant  $\sum_{n=1}^{\infty} \frac{\varepsilon_n}{3^n}$ , avec  $\varepsilon_n \in \{0, 2\}$ , a pour dimension  $\log 2 / \log 3$ .

**Encadré 2**

**MESURE BINOMIALE ALÉATOIRE**

Cette mesure est construite récursivement sur l'intervalle  $[0, 1]$  de la façon suivante. Soient  $a \in ]0, 1[$ ,  $b = 1 - a$ , et  $p \in ]0, 1[$ . On tire au hasard  $\mu([0, 1/2]) = a$  ou  $b$ , avec probabilité respectivement  $p$  et  $1 - p$ , et l'on prend  $\mu([1/2, 1]) = 1 - \mu([0, 1/2])$  ; une fois la mesure d'un intervalle dyadique  $\lambda$  déterminée, celle de son fils de gauche  $\lambda'$  est de même tirée au hasard et vaut  $\mu(\lambda') = a\mu(\lambda)$  ou  $(1 - a)\mu(\lambda)$  avec probabilité respectivement  $p$  et  $1 - p$  et celle de son fils de droite sera alors  $\mu(\lambda) - \mu(\lambda')$ . On construit ainsi par raffinements successifs une mesure de probabilité aléatoire sur  $[0, 1]$  dont on peut faire l'analyse

multifractale au sens suivant : l'exposant de Hölder d'une mesure  $\mu$  en un point  $x_0$  est défini par

$$H_\mu(x_0) = \liminf_{\delta \rightarrow 0} \frac{\log \mu([x_0 - \delta, x_0 + \delta])}{\log \delta}.$$

Le spectre de singularités est alors défini comme pour les fonctions. Le lien entre mesures multifractales et fonctions multifractales apparaît en dimension 1 et lorsque  $h < 1$  : l'exposant de Hölder d'une mesure positive  $\mu$  portée par  $[0, 1]$  coïncide avec l'exposant de Hölder de la fonction  $f(x) = \mu([0, x])$ .

Riemann, de nouveau, publiait en 1854 son fameux mémoire d'habilitation dans lequel est définie « l'intégrale de Riemann ». On savait depuis Cauchy définir l'intégrale de fonctions continues par morceaux ; aussi, pour montrer que cette nouvelle intégrale généralise effectivement l'intégrale de Cauchy, Riemann propose l'exemple de la fonction

$$\sum_{n=1}^{\infty} \frac{S(nx)}{n^2},$$

où  $S(x)$  est  $x$  auquel on soustrait l'entier le plus proche de  $x$ . On vérifie immédiatement que cette fonction est Riemann-intégrable et a cependant un ensemble dense de discontinuités ; elle n'est donc pas « Cauchy-intégrable ». Il s'agit ici encore d'une fonction multifractale ; son spectre de singularités est le segment  $D(h) = h$  pour  $h \in [0, 1]$ .

Plusieurs autres exemples, qui se révéleront ultérieurement être multifractals, balisent l'histoire de l'analyse au  $xx^e$  siècle. Les plus importants pour nous seront les *cascades multiplicatives*. L'exemple le plus simple en est la mesure binomiale (encadré 2). Des mesure aléatoires généralisant cette construction furent proposées par Mandelbrot en 1974 pour modéliser l'intermittence de la dissipation d'énergie d'un écoulement turbulent. L'étude mathématique de ces mesures fut réalisée par Kahane et Peyrière dès 1976. Ultérieurement, des modèles de cascade de plus en plus généraux et complexes furent proposés et étudiés. Il est vraiment remarquable que ces modèles, véritables cas d'école introduits en turbulence avant la notion de multifractal, se soient ensuite révélés être des exemples naturels d'une théorie dont les premiers succès ont effectivement été enregistrés dans le contexte de l'analyse de signaux en turbulence pleinement développée.

**Encadré 3**

**DÉCOMPOSITIONS EN ONDELETTES**

Une fonction  $\psi$  (régulière et bien localisée) engendre une base orthonormée d'ondelettes si les fonctions  $2^{j/2}\psi(2^j x - k)$  ( $j \in \mathbb{Z}$ ,  $k \in \mathbb{Z}$ ) forment une base orthonormée de  $L^2(\mathbb{R})$ .

Les coefficients d'ondelettes d'une fonction  $f$  sont alors les  $C_{j,k} = 2^j \int f(x)\psi(2^j x - k)dx$  (attention au fait que l'on n'utilise pas la normalisation  $L^2$ ).

Le coefficient  $C_{j,k}$  contient une information sur le comportement de  $f$  au voisinage de l'intervalle dyadique  $\lambda (= \lambda(j, k))$

$$= \left[ \frac{k}{2^j}, \frac{k+1}{2^j} \right] \text{ [près duquel l'ondelette est}$$

localisée. On note alors  $D_\lambda$  les suprema locaux

$$D_\lambda = \sup_{\lambda'(j',k') \subset \lambda} |C_{j',k'}|.$$

Si l'ondelette  $\psi$  est  $C^r$ , alors elle a ses  $r$  premiers moments nuls :  $\int \psi(x)dx = \int x\psi(x)dx = \dots = \int x^r \psi(x)dx = 0$ .

Si  $f$  se compose d'un comportement polynomial sur lequel est ajoutée une fluctuation, les coefficients d'ondelette font donc automatiquement abstraction de ce comportement polynomial (figure 1 sur l'ADN où cette propriété, spécifique aux ondelettes, est exploitée). La théorie des bases orthonormées d'ondelettes est essentiellement due aux travaux de Meyer, Mallat et Daubechies.

## QU'EST-CE QUE LE FORMALISME MULTIFRACTAL ?

Le calcul numérique du spectre de singularités d'un signal est clairement impossible à effectuer directement à partir de la définition (le calcul d'un exposant de Hölder qui peut être partout discontinu est déjà complètement instable numériquement). Les bases du formalisme multifractal ont été posées en 1985 par Parisi et Frisch dans le célèbre article où ils introduisent la notion même de multifractalité. Leur but était de calculer le spectre de singularités non pas directement à partir de sa définition, mais plutôt à partir de quantités auxiliaires facilement estimables numériquement. Ils proposaient de le faire à partir des fonctions de structure de la vitesse (normes  $L^p$  des accroissements de la vitesse) qui, depuis l'article fondateur de Kolmogorov sur la turbulence (1941), étaient des quantités couramment utilisées. La variante que nous allons exposer est basée sur une décomposition par ondelettes de la fonction. Elle constitue la caution mathématique des méthodes numériques (MMTO, ou méthode des maxima de la transformée en ondelettes) développées au début des années 90 par Arneodo et ses collaborateurs. L'intérêt d'utiliser les ondelettes est multiple, tant au niveau pratique (fiabilité et efficacité de la méthode MMTO) qu'au niveau théorique (nous verrons qu'elles permettent notamment de définir de nouveaux espaces fonctionnels sur lesquels sont basés les résultats mathématiques récents concernant le formalisme multifractal pour les fonctions). Pour simplifier la présentation, nous nous restreignons ici à des fonctions définies sur  $\mathbb{R}$ .

Le formalisme multifractal est basé sur la caractérisation suivante qui relie la régularité ponctuelle aux suprema locaux  $D_\lambda$  (encadré 3). Ce résultat est valable si  $f$  est uniformément hölderienne, c'est-à-dire s'il existe  $\varepsilon > 0$  et  $C > 0$  tels que

$$\forall x, y \quad |f(x) - f(y)| \leq C|x - y|^\varepsilon$$

(nous faisons cette hypothèse pour tous les résultats mathématiques qui suivent).

*L'exposant de Hölder de toute fonction  $f$  uniformément hölderienne est donné par*

$$H_f(x_0) = \liminf_{j \rightarrow +\infty, \lambda \in 3\lambda_j(x_0)} \frac{\log(D_\lambda)}{\log(2^{-j})} \quad (1)$$

(ici  $\lambda_j(x_0)$  désigne l'intervalle dyadique de côté  $2^{-j}$  contenant  $x_0$  et donc  $3\lambda_j(x_0)$  représente cet intervalle ainsi que les deux intervalles adjacents de même longueur).

Les quantités « globales » calculables sur un signal seront les valeurs de la fonction d'échelle définie, pour tout  $p \neq 0$ , par

$$\tau_f(p) = \liminf_{j \rightarrow +\infty} \frac{\log \left( \sum_{|\lambda|=2^{-j}} |D_\lambda|^p \right)}{\log(2^{-j})}, \quad (2)$$

où  $|\lambda|$  désigne la longueur de l'intervalle  $\lambda$  (on peut montrer que la fonction  $\tau_f(p)$  ne dépend pas de l'ondelette, suffisamment régulière, choisie). Le formalisme multifractal peut être établi de la façon suivante : on interprète (2) par le fait que

$$\sum |D_\lambda|^p \sim 2^{-\tau_f(p)j}.$$

Calculons la contribution à  $\sum |D_\lambda|^p$  des intervalles dyadiques de côté  $2^{-j}$  contenant un point où l'exposant de Hölder vaut  $h$  ; d'après (1), on a alors  $|D_\lambda| \sim 2^{-hj}$  et, par définition de la dimension, l'ensemble  $A_H$  est recouvert par  $\sim 2^{D(h)j}$  tels intervalles dyadiques. Cette contribution vaut donc

$$2^{(D(h)-ph)j}. \quad (3)$$

La contribution dominante sera celle correspondant à un  $h$  tel que l'exposant dans (3) est le plus grand possible. On s'attend donc à ce que

$$-\tau_f(p) = \sup_h (D(h) - ph).$$

Comme  $-\tau_f(p)$  est toujours une fonction convexe, si  $-D(h)$  est également convexe, alors  $-\tau_f$  et  $-D$  sont des fonctions convexes conjuguées qui se déduisent donc l'une de l'autre par transformation de Legendre-Fenchel, ce qui signifie que

$$D(h) = \inf_{p \in \mathbb{R}} (hp - \tau_f(p)) \quad (4)$$

qui est la formule recherchée. Empressons-nous de dire que le raisonnement heuristique ci-dessus est loin d'être une démonstration mathématique. Le seul résultat démontré en toute généralité est une majoration du spectre valable pour toute fonction :

$$D(h) \leq \inf_{p \in \mathbb{R}} (hp - \tau_f(p)).$$

Il existe de nombreux contre-exemples à (4) mais, en même temps, il est remarquable que cette formule se vérifie pour de nombreuses fonctions et processus aléatoires. Aujourd'hui, le but principal des recherches mathématiques en analyse multifractale est de comprendre son domaine de validité. A titre d'exemple, nous allons maintenant exposer un résultat de validité « générique » du formalisme multifractal.

**Encadré 4**

**LA PRÉVALENCE, UN « PRESQUE PARTOUT » EN DIMENSION INFINIE**

Dans un espace vectoriel  $E$  de dimension finie, la notion naturelle de « presque partout » invariante par translation signifie « hors d'un ensemble de mesure de Lebesgue nulle ». On vérifie facilement que, dans un espace de Banach de dimension infinie, il n'existe pas de mesure de Lebesgue (c'est-à-dire de mesure qui soit invariante par translation et qui prenne des valeurs finies non nulles sur les bornés d'intérieur non vide). On tourne cette difficulté en remarquant que, si  $E$  est de dimension finie, un borélien  $A \subset E$  est de mesure de Lebesgue nulle si et seulement s'il vérifie la propriété suivante :  
il existe une mesure de probabilité  $\mu$  à support compact telle que

$$\forall x \in E \quad \mu(x + A) = 0.$$

Cette caractérisation en dimension finie est prise comme définition si  $E$  est un espace vectoriel métrique complet de dimension infinie. Les ensembles  $A$  vérifiant cette propriété sont dits « Haar-nul ». Le complémentaire d'un ensemble « Haar-nul » est dit prévalent. Par abus de langage, on dira qu'une propriété qui est satisfaite (au moins) sur un ensemble prévalent a lieu presque partout. Les résultats suivants montrent que la notion de prévalence est une bonne généralisation de la notion de « presque partout » pour la mesure de Lebesgue :

- $A$  prévalent  $\implies \forall x \in E, x + A$  prévalent.
- $A$  prévalent  $\implies A$  dense.
- Une intersection dénombrable d'ensembles prévalents est un ensemble prévalent.

**VALIDITÉ PRÉVALENTE DU FORMALISME MULTIFRACTAL**

Remarquons tout d'abord que, si  $p$  est positif, la détermination de la fonction  $\tau_f(p)$  revient à savoir si  $f$  appartient ou non à certains espaces fonctionnels ; si  $s \in \mathbb{R}$  et  $p > 0$ , l'espace d'oscillations  $\mathcal{O}_p^s$  est défini par

$$\mathcal{O}_p^s = \{f : \forall j \geq 0, 2^{-j} \sum_{|\lambda|=2^{-j}} |D_\lambda|^p \leq C 2^{-spj}\}; \quad (5)$$

calculer  $\tau_f$  revient à écrire que

$$f \in \bigcap_{\varepsilon > 0, p > 0} \mathcal{O}_p^{\frac{\tau(p)+1}{p} - \varepsilon} \quad (6)$$

et

$$f \notin \bigcup_{\varepsilon > 0, p > 0} \mathcal{O}_p^{\frac{\tau(p)+1}{p} + \varepsilon}.$$

Notons  $\mathcal{O}^\tau$  l'espace défini par (6) ; c'est un espace vectoriel métrique complet. L'énoncé qui suit affirme que, au sens de la prévalence (encadré 3), presque toute fonction de  $\mathcal{O}^\tau$  est multifractale.

Presque toute fonction  $f$  de  $\mathcal{O}^\tau$  a pour fonction d'échelle

$$\tau_f(p) = \begin{cases} \tau(p) & \text{si } p > 0 \\ p\tau'(0) - 1 & \text{si } p < 0 \end{cases} \quad (7)$$

et satisfait le formalisme multifractal, c'est-à-dire vérifie (4).

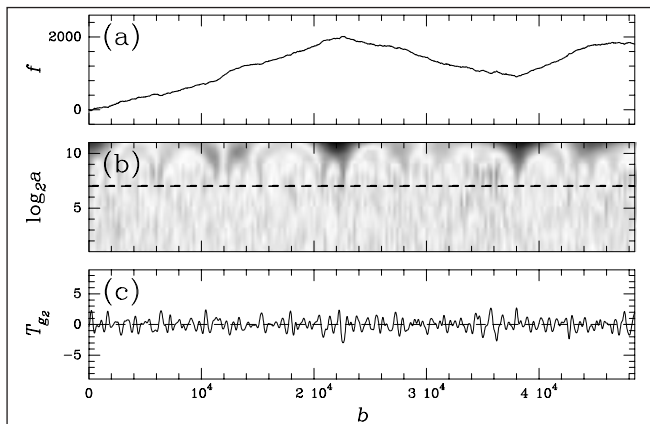
Mentionnons seulement le rôle clé joué ici par les ondelettes : le formalisme multifractal relie le spectre (défini à partir de quantités locales – les exposants de Hölder) à la fonction d'échelle (qui décrit des propriétés globales d'appartenance à des espaces fonctionnels) ; or, les ondelettes sont actuellement le seul système de représentation d'une fonction qui permette à la fois de caractériser ces propriétés locales [cf. (1)] et les espaces fonctionnels correspondants [cf. (5)].

La formule (1) appliquée aux fonctions d'échelle (7) fournit des spectres génériques qui ont une partie croissante concave puis valent  $-\infty$ . Le lecteur sera sans doute déçu de ne retrouver que la moitié gauche des courbes en  $\cap$  typiques dans les applications (figure 2 par exemple). En fait, l'utilisation d'espaces vectoriels, nécessaire dans le cadre de la prévalence, interdit de prendre en compte des  $p < 0$  dans la définition de l'espace  $\mathcal{O}^\tau$ . Or, la partie décroissante du spectre est obtenue dans (4) quand l'inf est atteint pour des  $p < 0$ . Le point de vue de la prévalence, par sa nature même, ne peut donner mieux. On ne sait pas si des spectres de singularités comme celui de la figure 2 peuvent être obtenus comme « spectres génériques » en un sens à préciser.

**L'ANALYSE MULTIFRACTALE DANS LES APPLICATIONS**

Lorsque l'on souhaite réaliser l'analyse multifractale d'un signal particulier, on est confronté au problème suivant : le spectre ne peut pas être calculé directement à

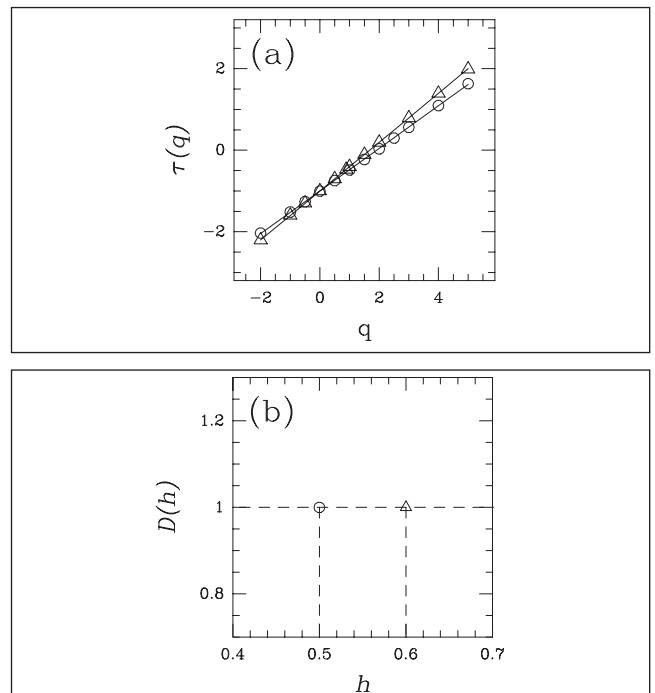




**Figure 1 - Analyse par ondelettes des séquences d'ADN**

Une séquence d'ADN est formée d'une chaîne dont chaque maillon est l'un des quatre acides nucléiques adénine (A), cytosine (C), guanine (G) et thymine (T). On lui associe une « marche ADN » (c'est-à-dire une fonction de  $\mathbb{R}^+$  dans  $\mathbb{Z}$  constante entre deux entiers consécutifs) en incrémentant de +1 chaque fois que l'on rencontre une purine (A ou G) et de -1 chaque fois que l'on rencontre une pyrimidine (C ou T). En (a) est représentée la marche ainsi obtenue pour la séquence du bactériophage  $\lambda$ . En (b) est illustrée la représentation espace-échelle fournie par la transformation en ondelettes continue en utilisant une ondelette analysatrice ayant deux moments nuls. On analyse ce signal à des échelles  $\geq 10$  nucléotides pour que les effets dus au caractère discret de la marche disparaissent. A très grande échelle, le signal est clairement affine par morceaux à cause de la composition hétérogène des génomes ; l'utilisation d'ondelettes ayant au moins deux moments nuls est donc nécessaire pour s'affranchir de ces tendances ; comme l'illustre la coupe (c) de la transformée en ondelettes effectuée à l'échelle  $\sim 400$  nucléotides, l'analyse par ondelettes permet alors d'étudier les propriétés d'invariance d'échelle des génomes.

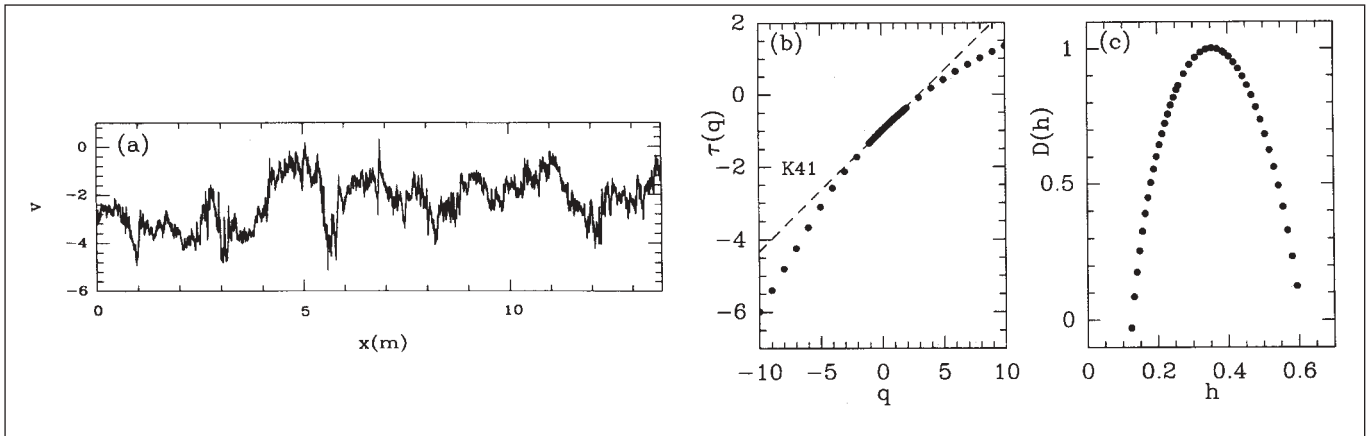
partir de sa définition et, d'autre part, les résultats mathématiques garantissant la validité « générique » du formalisme multifractal sont impuissants à fournir un résultat pour une fonction particulière. Il y a donc un acte de foi à appliquer le formalisme multifractal, même si les résultats mathématiques nous garantissent qu'il faudrait jouer de malchance pour qu'il ne soit pas vérifié, au moins pour la partie croissante du spectre (c'est-à-dire tant que l'inf est obtenu dans (4) pour des  $p$  positifs). Les figures 1 à 4 montrent quelques applications typiques de l'analyse multifractale effectuées avec la méthode MMTO, où la fonction d'échelle est désormais notée  $\tau(q)$ , en suivant la nomenclature utilisée dans les articles originaux de Arneodo *et al.* Dans chaque cas, on peut se demander ce que la connaissance du spectre de singularités apporte. La réponse dépend bien sûr de l'application et n'est que partiellement donnée (pour des raisons évidentes de concision) dans les figures. Ainsi, dans le domaine de la turbulence pleinement développée, nous avons vu que des modèles mathématiques (cascades multiplicatives) avaient été proposés pour modéliser une hypothétique structure multiplicative sous-jacente à la nature intermittente des fluctuations de vitesse et de dissipation d'énergie. L'analyse multifractale (figure 2) permet de déterminer les valeurs des paramètres de ces cascades pour que



**Figure 1 - (suite)**

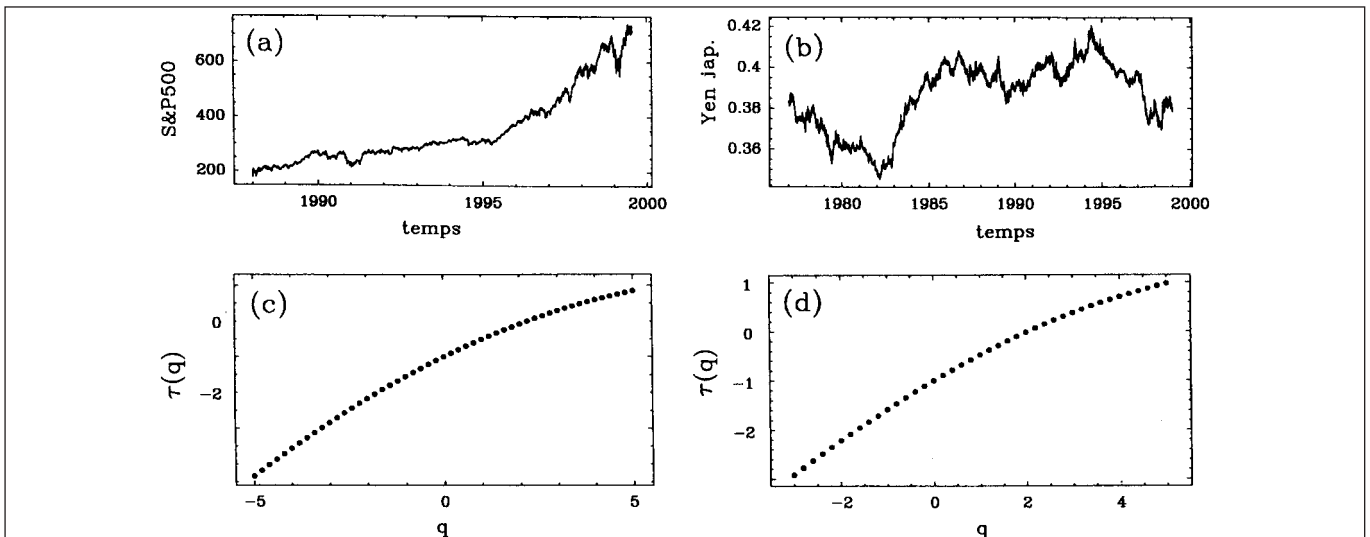
La figure (a) représente (cercles) la fonction d'échelle du bactériophage  $\lambda$ , et (triangles) la fonction d'échelle, moyennée sur 2 184 séquences, d'introns (partie ne codant pas pour les protéines) humains ; la figure (b) représente les spectres de singularités  $D(h)$  correspondants calculés par transformée de Legendre. On voit que les signaux correspondants ne présentent qu'un seul exposant de Hölder  $h \sim 0,6$  pour les introns, comme s'il s'agissait d'une fonction de Weierstrass ou d'un mouvement brownien fractionnaire corrélé à longue portée. On a en fait pu mettre en évidence des corrélations de ce type dans toutes les séquences d'ADN d'organismes eucaryotes (cellules possédant un noyau). Celles-ci permettent de comprendre la nature « multiéchelle » du mécanisme d'empaquetage de la double hélice dans le noyau. Dans le cas du bactériophage  $\lambda$  (et plus généralement dans l'ADN des cellules d'organismes procaryotes, c'est-à-dire qui ne possèdent pas de noyau), on observe un seul exposant de Hölder, mais qui vaut  $h = 0,5$  ; cela laisse supposer une absence de corrélations (par analogie avec la marche brownienne). L'analyse multifractale permet donc ici de différencier les séquences d'ADN de cellules possédant ou non un noyau.

le spectre de singularités du modèle coïncide avec le spectre expérimental ; il s'agit donc plus d'éliminer des modèles non satisfaisants que d'apporter la preuve expérimentale de la validité d'un modèle particulier certainement trop simpliste. Cette même analyse a permis également de détecter des événements rares tels que les passages occasionnels, près de la sonde, de fins filaments de vorticit  correspondant à un exposant de Hölder égal à  $-1$ . Ces filaments n'ont été mis en évidence expérimentalement que très récemment par le groupe de l'ENS dirigé par Couder. Ils échappent aux modèles de cascade et démontrent donc qu'une description réaliste des flots turbulents ne peut se limiter à un simple mécanisme de cascade à travers les échelles, aussi sophistiqué soit-il, mais qu'elle doit prendre également en compte les mécanismes de formation, d'interaction et de destabilisation de ces filaments de vorticit .



**Figure 2 - Signal de vitesse de turbulence pleinement développée**

Le signal représenté en (a) correspond à l'enregistrement ponctuel de la composante longitudinale du champ de vitesse par une sonde à fil chaud dans la soufflerie de l'ONERA à Modane. En (b), on voit que la fonction d'échelle  $\tau(q)$  diffère d'une fonction affine  $\tau(q) = qh - 1$  telle que celle obtenue (droite hachurée) pour un brownien fractionnaire (monofractal)  $B_{h=1/3}$  dont le spectre de puissance se comporte comme la fameuse loi en  $k^{-5/3}$  prédite par Kolmogorov pour les signaux de vitesse turbulents. Le spectre de singularités  $D(h)$  obtenu en (c) par transformation de Legendre s'étend entre les valeurs  $h_{min} = 0,12$  et  $h_{max} = 0,60$ . Les singularités hölderiennes du champ de vitesse jouent un rôle central pour comprendre la nature de la turbulence dans la mesure où ces variations de régularité du signal sont la manifestation de ce qui est couramment appelé « phénomène d'intermittence » en turbulence eulérienne.

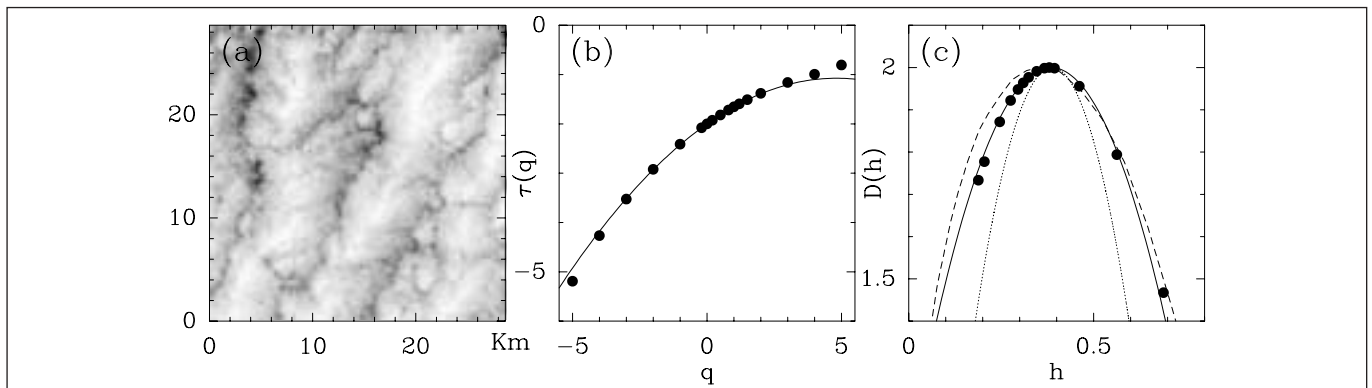


**Figure 3 - Analyse multifractale de signaux financiers**

La méthode MMTO a été appliquée à différents signaux financiers (taux de change, commodités, indices boursiers). On montre ici l'indice standard américain S&P500 (a) ainsi que le taux de change du yen par rapport au dollar américain (b). Le caractère non linéaire des fonction  $\tau(q)$  correspondantes montre que ces signaux sont multifractals. Ces résultats expérimentaux infirment les modèles classiques en finance basés sur le mouvement brownien (et ses variantes). La similarité des fonctions d'échelle obtenues avec celle observée pour les fluctuations de vitesse d'une particule dans un flot turbulent permet d'établir une analogie entre les finances et la turbulence dite lagrangienne : les signaux respectifs sont modélisables par une marche au hasard multifractale dont l'amplitude des pas est corrélée à longue portée alors que les signes sont quasiment décorrélés, ce qui explique les difficultés de prédiction.

Plus généralement, l'analyse multifractale est couramment utilisée comme aide à la modélisation (en calant les paramètres d'un modèle à l'aide du spectre de singularités numériquement calculé ou, éventuellement, en réfutant le modèle). Elle peut aussi être une étape indispensable à la synthèse. C'est également un outil de *classification*, en analyse de texture par exemple. Ainsi récemment, les premières applications de la méthode MMTO à l'imagerie mammographique ont conduit à classifier les fluctuations de régularité de mammogrammes de seins normaux suivant la nature grasse ou glandulaire du tissu mammaire. L'étude de seins anor-

maux a permis de détecter et d'identifier les microcalcifications comme des singularités fortes (d'exposant de Hölder égal à  $-1$ ) relativement aux singularités présentes dans les fluctuations de rugosité de la structure du sein ; de plus, la décomposition espace-échelle que fournit la décomposition en ondelettes 2D permet naturellement de regrouper les microcalcifications en amas dont les propriétés géométriques sont essentielles pour distinguer les microcalcifications de nature maligne de celles de nature bénigne. Ainsi, cette méthode se révèle être une approche très prometteuse pour l'aide au diagnostic en imagerie médicale.



**Figure 4 - Analyse d'images satellite de nuages**

Un nombre important de phénomènes naturels comme de laboratoire conduisent à la formation de surfaces rugueuses très irrégulières. La méthode MMTO a été généralisée en dimension 2 par Arneodo et ses collaborateurs. Nous présentons l'analyse d'une image prise à partir du satellite Landsat d'un stratocumulus marin (a). Les nuages ont une influence non négligeable sur la propagation du rayonnement solaire dans l'atmosphère ; ils jouent donc un rôle central dans la régulation du climat. De ce fait, la modélisation de leur structure est primordiale pour prédire l'évolution des conditions climatiques. L'extrême simplicité des modèles utilisés actuellement pour simuler la composante nuage dans le problème de l'interaction nuage-rayonnement est responsable pour une grande part de l'incertitude des modèles climatiques. La nature multifractale des images de nuages est clairement mise en évidence par les résultats du calcul de la fonction d'échelle (b) et du spectre de singularités (c) qui sont remarquablement reproduits par les prédictions d'un modèle de cascade log-normale (trait plein). La comparaison du spectre obtenu avec ceux calculés pour la vitesse (ligne pointillée) et la température (ligne hachurée) dans un champ turbulent suggère que la distribution spatiale des gouttelettes d'eau dans un nuage est l'empreinte statistique de la nature intermittente de la turbulence atmosphérique. Enfin, on voit que des cascades multiplicatives simples pourraient fournir un outil de modélisation infiniment meilleur que les modèles très rudimentaires (constants par morceaux) utilisés actuellement dans l'étude de l'interaction entre les nuages et le rayonnement solaire.

Les résultats mathématiques récents ont eu un profond impact dans les domaines appliqués. Ainsi, les physiciens pensaient encore récemment qu'un comportement multifractal était la signature d'une organisation interne extrêmement précise dans le signal (phénomènes de cascade, autosimilarité...). Les résultats mathématiques de généralité ont renversé cette perspective, puisqu'ils montrent qu'un signal quelconque est, en général, multifractal.

Ces avancées mathématiques ne répondent pas à toutes les questions des utilisateurs : on a vu que la prévalence

est, par nature, incapable de conforter l'expérimentateur par un résultat de validité « générique » portant sur tout le spectre calculé. De plus, l'exposant de Hölder donne une information très incomplète sur la nature de la singularité en un point. Les applications demandent aujourd'hui une classification beaucoup plus fine de ces singularités, prenant en compte les comportements oscillatoires et (en dimension 2 et plus) les comportements directionnels ; il faudra alors construire une nouvelle analyse multifractale adaptée à cette nouvelle classification.

#### POUR EN SAVOIR PLUS

**Abry (P.), Gonçalves (P.), Lévy-Véhel (J.) Eds.,** *Lois d'échelle, fractales et ondelettes*, Lavoisier (Coll. Hermes), 2002.

**Arneodo (A.), Argoul (F.), Bacry (E.), Elezgaray (J.), Muzy (J.-F.),** *Ondelettes, multifractales et turbulence : de l'ADN aux croissances cristallines*, Diderot Editeur, Arts et Sciences, Paris, 1995.

**Arneodo (A.), Audit (B.), Decoster (N.), Muzy (J.-F.), Vaillant (C.),** *Wavelet-based multifractal formalism: applications to DNA sequences, satellite images of the cloud structure and stock market data*, dans : « The Science of Disasters », A. Bunde, J. Kropp, H.-J. Schellnhuber eds., Springer, p. 27-102, 2002.

**Arneodo (A.), Bacry (E.), Muzy (J.-F.),** *The thermodynamics of fractals revisited with wavelets*, Physica A, Vol. 213, p. 232-275, 1995.

**Hunt (B.), Sauer (T.), Yorke (J.),** *Prevalence: A translation invariant 'almost every' on infinite dimensional spaces*, Bull. AMS, Vol. 27, p. 217-238, 1992.

**Jaffard (S.),** *Wavelet techniques in multifractal analysis*, à paraître dans : « Fractal Geometry and Applications: A Jubilee of Benoît Mandelbrot », M. Lapidus ed. Proceedings of Symposia in Pure Mathematics.

**Jaffard (S.), Meyer (Y.), Ryan (R.),** *Wavelets: Tools for Science and Technology*, S.I.A.M., 2001.

**Muzy (J.-F.), Bacry (E.), Arneodo (A.),** *The multifractal formalism revisited with wavelets*, Int. J. Bif. Chaos, Vol. 4, p. 245-302, 1994.

# Intégrabilité de systèmes hamiltoniens

**Le mouvement d'une toupie, celui d'un pendule sphérique, avec leur régularité et leur presque périodicité, appartiennent au monde des systèmes intégrables. Peut-on démontrer que tel ou tel système, apparemment plus chaotique (problème des trois corps, système de Hénon-Heiles...), n'est pas intégrable ? Oui, grâce à un théorème de Morales et Ramis. L'outil ? La théorie de Galois différentielle.**

Un système hamiltonien est un système mécanique régi par les équations de Hamilton

$$\dot{q}_1 = \frac{\partial H}{\partial p_1}, \dots, \dot{q}_n = \frac{\partial H}{\partial p_n},$$

$$\dot{p}_1 = -\frac{\partial H}{\partial q_1}, \dots, \dot{p}_n = -\frac{\partial H}{\partial q_n}.$$

L'énergie totale  $H$  d'un tel système, fonction des grandeurs  $q_1, \dots, q_n$  (penser à des positions) et  $p_1, \dots, p_n$  (penser à des impulsions), est conservée au cours du temps.

Il arrive que d'autres quantités que l'énergie soient conservées, elles aussi. On les appelle des intégrales premières.

S'il y en a assez (qui commutent, en un sens que je ne veux pas préciser ici), Liouville a démontré au XIX<sup>e</sup> siècle que l'on peut résoudre le système différentiel par des quadratures (en calculant des intégrales). C'est pourquoi on dit que le système est complètement intégrable.

Il y a de nombreux exemples de systèmes hamiltoniens complètement intégrables. Commençons par les deux plus classiques :

## LA TOUPIE

Tout le monde a déjà vu et touché une toupie (sinon, en voici une – voir la figure 1).

On considère ici que c'est un solide avec un point fixe (celui où la toupie est en contact avec le plan horizontal, le point  $O$  de la figure) soumis à la seule pesanteur. Ce solide a un axe de révolution. Le système mécanique a été étudié par Lagrange à la fin du XVIII<sup>e</sup> siècle. En plus

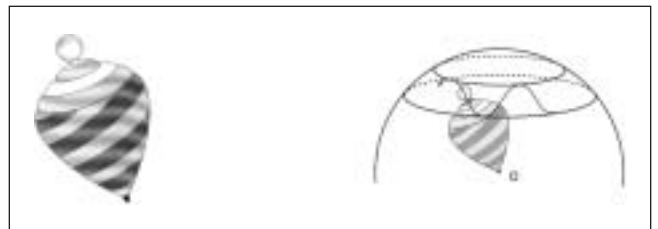


Figure 1 - Mouvement de l'axe d'une toupie.

de l'énergie totale, il y a évidemment une deuxième quantité conservée, le moment par rapport à l'axe de symétrie.

Comme tous les enfants le savent, l'extrémité de l'axe de révolution oscille entre deux parallèles de la sphère centrée au point fixe, comme indiqué sur la figure.

## LE PENDULE « SPHÉRIQUE »

Il s'agit d'un pendule, suspendu à un point fixe  $O$  par une tige rigide, et soumis, lui aussi, à la seule pesanteur. Il y a encore une deuxième intégrale première « évidente », le moment par rapport à la verticale.

La boule tourne autour de l'axe vertical tout en oscillant entre deux petits cercles parallèles de la sphère. La figure ci-dessous représente la projection d'une trajectoire sur un plan horizontal.

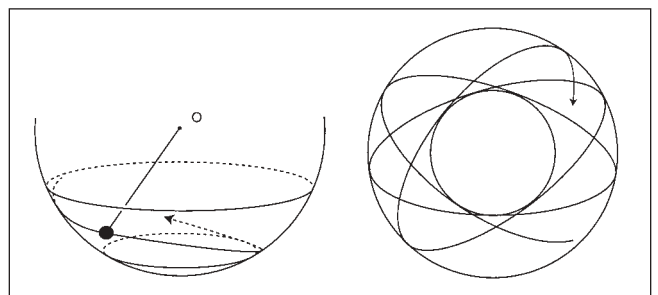


Figure 2 - Le pendule sphérique.

## GÉODÉSQUES

On aura remarqué la similitude des deux situations précédentes. Des comportements analogues (oscillation dans une bande) apparaissent dans de nombreux autres problèmes de mécanique, comme, par exemple, le mouvement d'une particule libre sur une surface de révolution ou sur un ellipsoïde.

Une particule libre va au plus court et suit une géodésique. Les figures ci-dessous représentent une géodésique d'une surface de révolution et d'un ellipsoïde respectivement.

Dans le cas de la surface de révolution, le moment de la particule par rapport à l'axe de révolution est une intégrale première. Pour un ellipsoïde « quelconque » (pas de révolution), c'est moins évident, mais il y a aussi une « deuxième » intégrale première (Jacobi, 1838, Uhlenbeck, 1980).

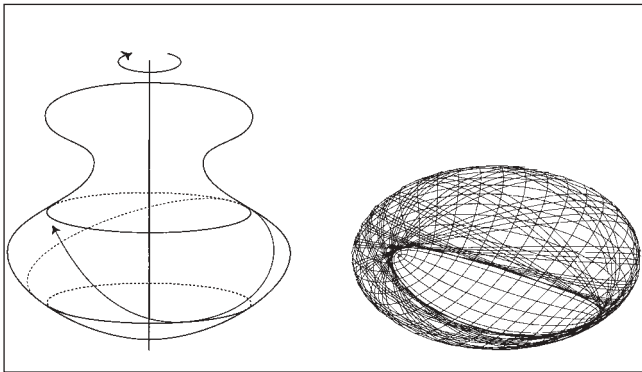
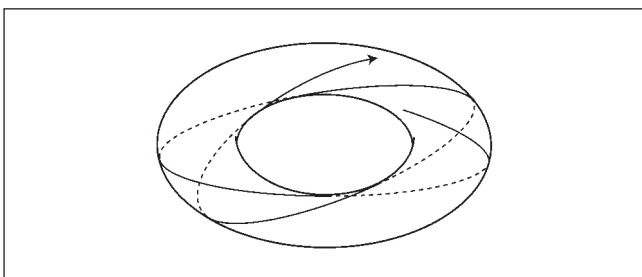


Figure 3 - Géodésiques d'une surface de révolution, d'un ellipsoïde.

## DES BANDES ET DES TORES

Une expression géométrique ou dynamique de l'intégrabilité à la Liouville est la régularité des solutions. Le mouvement décrit par un système hamiltonien intégrable est extrêmement régulier. Les trajectoires s'enroulent sur des tores (c'est le théorème dit d'Arnold-Liouville), chacune revenant régulièrement près de son point initial, on dit que le mouvement est « quasi périodique ».

C'est ce que montre la figure ci-dessous, que l'on peut imaginer dessinée dans l'espace de phases (en volume, sur un tore) ou dans l'espace de configuration (à plat,



comme sur la feuille de papier) où elle ressemble beaucoup aux figures précédentes.

## LES SYSTÈMES HAMILTONIENS SONT-ILS TOUS INTÉGRABLES ?

On l'a vu, la physique peut fournir des intégrales premières, comme le moment par rapport à un axe de révolution (toupie, pendule sphérique, particule libre sur une surface de révolution...).

Il y a aussi beaucoup de systèmes hamiltoniens qui ne sont pas intégrables.

## LE PROBLÈME A $n$ CORPS

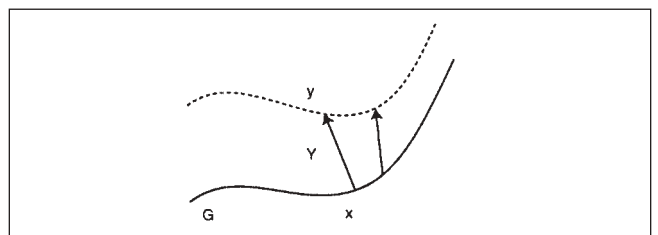
Le plus célèbre est le problème « de la Lune » (problème de trois corps en interaction gravitationnelle). On sait que le problème à deux corps (Soleil-Terre) est intégrable. C'est même pour l'intégrer que Lagrange a introduit les prémisses de la géométrie symplectique et de la mécanique hamiltonienne. Poincaré a démontré que le problème à trois corps ne pouvait avoir assez d'intégrales premières *analytiques*, c'est-à-dire qui peuvent s'écrire comme des sommes (éventuellement infinies) de momomes faisant intervenir les positions et les moments des trois corps. La méthode que je présente ici permet de montrer qu'il n'en a pas assez, même si on autorise les éventuelles intégrales à ne plus être tout à fait analytiques, mais à avoir des dénominateurs (des pôles, on dit qu'elles sont méromorphes).

Il y a des systèmes hamiltoniens dont on soupçonne qu'ils ne sont pas intégrables, parce que l'on n'a pas été capable de leur trouver assez d'intégrales premières, et surtout parce que des expériences ou simulations numériques montrent un comportement chaotique incompatible avec le théorème d'Arnold-Liouville (figure de l'encadré 1).

## LE GROUPE DE GALOIS, UNE OBSTRUCTION A L'INTÉGRABILITÉ

Selon une tradition remontant à la *Mécanique céleste* de Poincaré, on considère l'équation aux variations, décrivant les solutions « infinitésimalement proches » d'une solution donnée. Je vais expliquer ceci de façon heuristique, puis je donnerai un exemple.

## LES TRAJECTOIRES INFINIMENT PROCHES



On choisit une trajectoire (une solution du système différentiel)  $x(t)$  et on écrit que  $y(t)$  est aussi une solution, très proche, de sorte que l'on peut écrire  $y(t) = x(t) + Y(t)$  et que, à l'ordre 1, notre système différentiel devient linéaire en  $Y$  : on a, à l'ordre 1,

$$\begin{aligned} \dot{Y} &= \dot{y} - \dot{x} \\ &= X(y(t)) - X(x(t)) \\ &= (dX)_{x(t)}(Y(t)). \end{aligned}$$

Cette équation différentielle *linéaire* en  $Y$  est l'équation aux variations.

**L'EXEMPLE DE HÉNON-HEILES**

Dans le cas simple considéré dans l'encadré 1, le système différentiel est

$$\begin{aligned} \dot{q}_1 &= p_1, & \dot{q}_2 &= p_2, \\ \dot{p}_1 &= 2q_1q_2, & \dot{p}_2 &= q_1^2. \end{aligned}$$

**Encadré 1**

**LE SYSTÈME DE HÉNON-HEILES**

Étant donné un système hamiltonien, il n'est pas facile en général de décider s'il est, ou s'il n'est pas, intégrable. Je vais essayer d'illustrer cette remarque à l'aide du système de Hénon-Heiles.

C'est le système défini par le hamiltonien<sup>a</sup>

$$H = \frac{1}{2}(p_1^2 + p_2^2) + \frac{1}{2}(Aq_1^2 + Bq_2^2) - q_1^2q_2 - \frac{\lambda}{3}q_2^3$$

où  $A$ ,  $B$  et  $\lambda$  sont des paramètres à préciser.

Le système différentiel des équations de Hamilton est

$$\begin{aligned} \dot{q}_1 &= p_1 \\ \dot{q}_2 &= p_2 \\ \dot{p}_1 &= -Aq_1 + 2q_1q_2 \\ \dot{p}_2 &= -Bq_2 + q_1^2 + \lambda q_2^2. \end{aligned}$$

Il existe des valeurs des paramètres pour lesquelles on sait que ce système est intégrable.

– C'est le cas quand  $A = B$  et  $\lambda = 1$ . Le hamiltonien s'écrit

$$H = \frac{1}{2}(y_1^2 + y_2^2) + Ax_1^2 - \frac{4}{3}x_1^3 + Ax_2^2 + \frac{4}{3}x_2^3$$

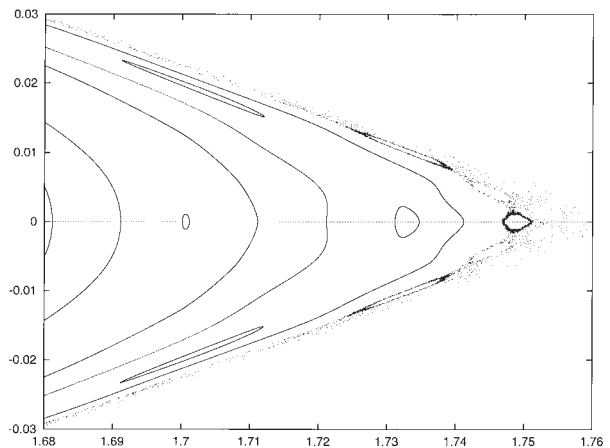
(où  $x_1 + x_2 = q_1$ ,  $x_1 - x_2 = q_2$  et les  $y_i$  sont les moments correspondants) de sorte que la fonction

$$K = \frac{1}{2}y_1^2 + Ax_1^2 - \frac{4}{3}x_1^3$$

est une intégrale première.

– Plus mystérieusement, quand  $\lambda = 6$ , la fonction  $K$  définie par Bountis, Segur et Vivaldi et par

$$\begin{aligned} K &= q_1^4 + 4q_1^2q_2^2 + 4p_1(p_1q_2 - p_2q_1) \\ &\quad - 4Aq_1^2q_2 + (4A - B)(p_1^2 + Aq_1^2) \end{aligned}$$



est une intégrale première pour le hamiltonien de Hénon-Heiles.

La figure ci-dessus montre une partie de la dynamique (de l'application de Poincaré, pour être précise) du système de Hénon-Heiles pour  $A = B = 0$  et  $\lambda = 3/2$ . Sans entrer dans les détails, elle semble indiquer que ce système est trop chaotique pour entrer dans la famille des systèmes présentés au début de cet article.

La méthode que je vais présenter permet de montrer qu'en effet, le système de Hénon-Heiles n'est pas intégrable en général.

Dans cet article, je ne considérerai que le cas simple où  $A = B = 0$  et  $\lambda = 0$ , c'est-à-dire où

$$H = \frac{1}{2}(p_1^2 + p_2^2) - q_2q_1^2.$$

<sup>a</sup> Ce hamiltonien sert notamment à modéliser le mouvement d'une étoile dans une galaxie cylindrique.

Parmi ses solutions, il y en a de très simples, les droites paramétrées par

$$q_1 = 0, \quad p_1 = 0,$$

$$q_2(t) = at - b, \quad p_2(t) = a$$

où  $a$  et  $b$  sont des constantes d'intégration arbitraires. L'équation aux variations le long d'une de ces solutions est le système différentiel linéaire

$$\begin{aligned} \dot{Q}_1 &= P_1 \\ \dot{Q}_2 &= P_2 \\ \dot{P}_1 &= 2q_2(t)Q_1 \\ \dot{P}_2 &= 0 \end{aligned}$$

obtenu en linéarisant le système hamiltonien.

On se contente d'en étudier les solutions vérifiant  $Q_2 = P_2 = 0$ . Le système linéaire  $\dot{Q}_1 = P_1$ ,  $\dot{P}_1 = 2q_2(t)Q_1$  est équivalent à l'équation différentielle

$$\ddot{Q} - 2(at - b)Q = 0.$$

C'est une équation d'Airy, équation dont les solutions, les « fonctions d'Airy », sont des fonctions analytiques sur le plan complexe tout entier, mais dont aucune solution n'est une fraction rationnelle (quotient de deux polynômes) ni même une fonction algébrique (par exemple racine de fraction rationnelle). Pour ceux ou celles qui aiment les formules, on peut les écrire

$$Q(t) = \int_0^\infty \cos(x^3 \pm xt) dx.$$

## Encadré 2

# LA THÉORIE DE GALOIS

Ouvrons ici une parenthèse.

Supposons que l'on ne connaisse que les nombres rationnels et que l'on ait affaire à une équation algébrique. Il se peut qu'elle n'ait pas de solution rationnelle. C'est le cas, par exemple, pour  $x^2 - 2 = 0$  dont les solutions  $\sqrt{2}, -\sqrt{2}$ , sont des nombres irrationnels. Pour travailler avec les solutions de l'équation, on a besoin de considérer un ensemble de nombres plus gros, dans lequel on puisse calculer comme avant et qui contienne les vieux nombres (rationnels) ainsi que les solutions de l'équation.

Dans la théorie de Galois, on considère les transformations qui permutent ces nouveaux nombres (en fixant les anciens). Ces transformations forment un groupe. Dans l'exemple, on peut seulement échanger  $\sqrt{2}$  et  $-\sqrt{2}$ , le groupe de Galois est un groupe à deux éléments, formé de la transformation qui fixe  $\sqrt{2}$  et  $-\sqrt{2}$  (transformation identique) et de celle qui les échange.

Un des premiers succès de la théorie de Galois est d'avoir pu montrer qu'une équation algébrique

$$x^n + a_1x^{n-1} + \dots + a_n = 0$$

est résoluble par radicaux, c'est-à-dire par des formules telles que

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

pour les équations du second degré ou

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} - \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

pour l'équation

$$x^3 + px + q = 0,$$

que cette équation, donc, est résoluble par radicaux si et seulement si son groupe de Galois est... résoluble (justement !), c'est-à-dire peut se dévisser en morceaux qui sont tous des groupes commutatifs. Par exemple, pour une équation assez générale de degré 5 ou plus, le groupe de Galois n'est pas résoluble, il est donc inutile de chercher des formules analogues à celles que je viens d'écrire pour les équations de ces degrés.

Comme les équations algébriques, les équations différentielles linéaires ont un groupe de Galois. Supposons que les coefficients d'un système différentiel linéaire soient, comme dans notre exemple, des fractions rationnelles. Il se peut que les solutions soient, elles, beaucoup plus compliquées, comme on l'a vu dans l'exemple de l'équation d'Airy. A l'arsenal de fonctions dont nous sommes partis, on ajoute donc de nouvelles fonctions.

Le groupe de Galois (différentiel) est le groupe des transformations de cet ensemble de fonctions qui fixent les fractions rationnelles. Dans le cas d'une équation différentielle d'ordre 2, c'est un groupe de matrices  $2 \times 2$ . Dans le cas d'Airy, les solutions (et plus précisément leur comportement à l'infini) sont assez compliquées pour que le groupe de Galois soit très gros. C'est le groupe de toutes les matrices de déterminant 1. Refermons la parenthèse.

### LE THÉORÈME DE MORALES ET RAMIS

Le groupe de Galois différentiel (encadré 2) est l'acteur principal d'un théorème de non-intégrabilité dû à Morales et Ramis, dans une lignée de travaux remontant à Kowalevskaya (voir ci-dessous), Poincaré, Painlevé et plus récemment Ziglin. Ce théorème peut être considéré comme un analogue du théorème sur la résolubilité des équations algébriques que j'ai mentionné dans l'encadré 2. Il affirme que, *si un système hamiltonien est intégrable, alors le groupe de Galois du système différentiel linéarisé le long de n'importe quelle solution doit être presque commutatif*, au sens où, à un groupe fini près, il est commutatif<sup>1</sup>.

Concrètement (si j'ose dire) : vous choisissez une solution, vous linéarisez le système le long d'icelle, vous calculez le groupe de Galois, s'il n'est pas (presque) commutatif, vous pouvez conclure que le système n'était pas intégrable.

Encore faut-il avoir trouvé une solution, à la fois assez simple pour que vous ayez été capable de calculer le groupe de Galois et assez compliquée pour que celui-ci ne soit pas (presque) commutatif.

Toujours est-il que dans le cas simple considéré ici, le groupe de Galois est le groupe des matrices de déterminant 1, qui n'est pas commutatif et même pas presque commutatif, ce qui permet de conclure à la non-

intégrabilité du système de Hénon-Heiles dans le cas considéré.

### CONCLUSION

La toute première approche à la non-intégrabilité est due à S. Kowalevskaya en 1889. Elle étudiait l'intégrabilité du système hamiltonien décrivant le mouvement d'un solide avec un point fixe dans un champ de pesanteur constant. Elle s'est demandé à quelle condition les solutions du système sont des fonctions *méromorphes*<sup>2</sup> du temps, c'est-à-dire que leurs seules singularités sont des pôles (pas de ramification, logarithme, etc).

Elle a démontré que cette propriété n'est satisfaite que dans trois cas, ceux d'un solide mobile autour de son centre de gravité ou d'un solide avec un axe de révolution (la toupie), où l'on savait que le système était intégrable au sens utilisé dans ce texte, et un nouveau cas, qui porte depuis son nom et dont elle a montré qu'il était, lui aussi, intégrable, en exhibant l'intégrale première manquante.

La relation entre l'intégrabilité (au sens dit « de Liouville ») et la douceur des singularités des solutions n'est toujours pas complètement élucidée (voir par exemple le livre de Zakharov cité ci-après). Les méthodes d'algèbre différentielle que j'ai présentées ici s'en approchent – à l'ordre 1.

### POUR EN SAVOIR PLUS

Sur le théorème d'Arnold-Liouville :

**Arnold (V.I.)**, « Méthodes mathématiques de la mécanique classique », *Mir*, Moscou, 1974.

Sur le théorème de Morales et Ramis :

**Morales-Ruiz (J.)**, « Differential Galois theory and non-integrability of Hamiltonian systems », *Progress in Math.*, *Birkhäuser*, 1999.

**Audin (M.)**, « Les systèmes hamiltoniens et leur intégrabilité », *Cours Spécialisés*, 8, *Société mathématique de France & EDP Sciences*, 2001.

Sur la notion d'intégrabilité :

**Kowalevski (S.)**, « Acta Math. », 12, 1889, 177.

**Zakharov (V.E.)**, éditeur, « What is integrability? », *Springer*, Berlin, 1991.

Sur la notion de plagiat par anticipation :

**Le Lionnais (F.)**, « Le second manifeste (1973), La bibliothèque oulipienne 2 », *Ramsay*, Paris, 1987.

<sup>1</sup> Si on néglige les groupes finis, cette propriété est beaucoup plus forte pour un groupe que d'être résoluble. A l'origine, ce que Morales et Ramis pensaient montrer, c'était la (presque) *résolubilité* de leurs groupes de Galois.

<sup>2</sup> C'est ce que l'on appelle aujourd'hui la « propriété de Painlevé » ou le « test » de Painlevé (sans doute un *plagiat par anticipation* de la part de Kowalevskaya).

### Note de l'auteur

La toupie utilisée dans les figures a été dessinée par Raymond Seroul. La figure illustrant l'encadré 1 est extraite du livre de Juan Morales et m'a été prêtée par son auteur. Qu'ils soient remerciés, ainsi que les lecteurs anonymes qui m'ont aidée à améliorer la rédaction de versions préliminaires de cet article.



# Sur la forme de certains espaces provenant de constructions arithmétiques

**Un théorème classique de Fermat affirme que toute équation du type  $m^2 - an^2 = \pm 1$ , où  $a$  est un entier sans facteurs carrés, admet une infinité de solutions entières  $(m, n)$ .**

**On peut voir ce résultat comme un cas très particulier d'un théorème de Borel et Harish-Chandra concernant la finitude du volume de certains espaces obtenus par des constructions arithmétiques.**

**Ces résultats sont décrits ici dans leur contexte géométrique et l'on tente d'esquisser un début d'étude de la forme de ces espaces.**



« Flight in Klein space » par J. Weeks (extrait de sa page web <http://www.geometrygames.org/ESoS/index.html>).

## LES ESPACES SYMÉTRIQUES

A sa naissance comme théorie mathématique, la géométrie est une et régie par cinq postulats : les axiomes d'Euclide. Au XIX<sup>e</sup> siècle, cette unité est bouleversée par les développements de la géométrie projective de Desargues et Pascal, et par la découverte par Bolyai, Gauss,

---

– Nicolas Bergeron, laboratoire de mathématiques d'Orsay  
– UMR 8628 CNRS – Université Paris-Sud, bâtiment 425,  
91405 Orsay cedex.  
[Nicolas.Bergeron@math.u-psud.fr](mailto:Nicolas.Bergeron@math.u-psud.fr)

Lobatchevski et Riemann de nouvelles géométries ne satisfaisant pas au cinquième axiome d'Euclide, les géométries non euclidiennes. Ces changements amènent le mathématicien Klein, sous l'influence de son ami Lie, à penser chaque géométrie comme associée à un objet primordial : un **groupe** (encadré 1).

Le groupe sous-jacent à une géométrie est une sorte de codage des symétries de cette géométrie. Dans le cas de la géométrie euclidienne, il est en gros constitué des rotations et des translations de l'espace euclidien. Chaque groupe est vu par Klein comme opérant sur un ensemble, l'espace euclidien dans le cas de la géométrie classique. La fécondité de cette idée est immédiatement illustrée par Klein en établissant l'isomorphie, *i.e.* l'équivalence abstraite, de géométries d'allures toutes différentes.

Au cours de ce même XIX<sup>e</sup> siècle, Riemann étend lui aussi le domaine de la géométrie en proposant un point de vue totalement différent. Alors que pour Klein la beauté des nouvelles géométries non euclidiennes provient de l'existence d'un groupe de symétries qui permet de déplacer arbitrairement une figure rigide, Riemann considère des espaces plus généraux, dans lesquels les mouvements d'un corps rigide ne sont pas nécessairement possibles. En général par exemple, dans la géométrie de Riemann on ne peut pas déplacer un triangle sans en déformer les longueurs et les angles. Schématisons en disant que Klein étend la notion de géométrie en touchant aux transformations, ou aux symétries, alors que Riemann s'attaque à l'espace.

Cette modification de l'espace par Riemann engendre la notion de **variété différentiable** (encadré 2). Celle-ci permet de modéliser la notion de grandeur variable

pluridimensionnelle. Les exemples les plus simples sont les espaces des paramètres d'un système mécanique, comme par exemple l'espace des positions d'un corps solide.

La deuxième idée de Riemann consiste à définir la mesure des longueurs à partir d'un élément de longueur infinitésimal qui, lui, peut être transporté d'un point à un autre. Une variété différentiable munie d'une telle distance est depuis lors appelée *variété riemannienne*.

La notion de variété riemannienne est très flexible dans le choix de l'élément de longueur (ce qui, en général, rend le déplacement d'un corps rigide impossible). Cette flexibilité explique le grand rôle que les variétés riemanniennes jouent en physique, notamment dans la relativité générale d'Einstein.

Certaines de ces variétés riemanniennes sont beaucoup plus symétriques que les autres : elles ont un « gros » groupe de transformations qui préservent la distance, transformations appelées *isométries*. La recherche frénétique de la symétrie étant la principale névrose des mathématiciens, ces *espaces symétriques* prennent rapidement une place centrale dans la géométrie, sous l'impulsion de Cartan. Ils ont en effet la particularité de synthétiser les points de vue de Klein et de Riemann et contiennent comme cas particulier les géométries euclidiennes et non euclidiennes que l'on a évoquées au premier paragraphe.

Voyons quel sens Cartan donne à l'expression « avoir un gros groupe d'isométries ». On dit qu'une variété

riemannienne  $X$  est un *espace symétrique* si, pour tout point  $x$  dans  $X$ , il existe une isométrie de  $X$  qui fixe le point  $x$  mais bouge tous les points suffisamment proches de  $x$  (mais différents de  $x$  !). Puisque  $X$  a beaucoup de points (c'est un espace continu) le groupe de ses isométries est « gros » : il est infini et, en tant qu'espace, il est lui aussi continu. C'est un groupe de Lie (encadré 1). De la définition ci-dessus, il découle que si  $X$  est un espace symétrique et  $G$  le groupe de toutes ses isométries, un point arbitraire de  $X$  peut être bougé par un élément de  $G$  vers n'importe quel autre point de  $X$  ; on dit alors que l'action est transitive (encadré 1). Comme nous l'annonçait Klein, l'objet primordial est bien le groupe : on peut retrouver l'espace  $X$  à partir du seul groupe  $G$ .

Néanmoins, la confrontation avec le point de vue riemannien est extrêmement féconde et justifie la place centrale qu'occupent actuellement les espaces symétriques en mathématique, à l'intersection de l'algèbre, de l'analyse et de la géométrie.

Il est facile de vérifier que la sphère et l'espace euclidien sont des espaces symétriques : il suffit de considérer les rotations autour de chaque point. Un autre exemple, fondamental, d'espace symétrique est le **plan hyperbolique** (encadré 3), modèle de la géométrie non euclidienne de dimension 2, découverte par Bolyai, Lobatchevski et Gauss.

### Encadré 1

## GROUPES

*Les points d'un plan peuvent être transformés en d'autres points par des rotations, des translations... Dans un registre différent, les cartes d'un jeu de cartes peuvent être permutées de diverses manières. Derrière ces différentes opérations se cache un même concept dégagé par Galois, le concept de groupe agissant sur un ensemble : le groupe des rotations ou le groupe des rotations-translations agissent sur le plan, le groupe des permutations agit sur l'ensemble des cartes. Un groupe est un ensemble  $G$  muni d'une loi notée « . » qui, à deux éléments  $g_1$  et  $g_2$  de  $G$ , associe un troisième élément  $g_1.g_2$  de  $G$ . On demande de plus à cette loi de vérifier les deux propriétés suivantes :*

- 1. il existe un élément  $e$  dans  $G$  tel que pour tout élément  $g$  dans  $G$ , on ait  $e.g = g.e = g$  ; cet élément est appelé élément neutre ;*
- 2. pour tout élément  $g$  de  $G$ , il existe un élément  $h$  dans  $G$  tel que  $g.h = h.g = e$  ; on appelle  $h$  l'inverse de  $g$  et on le note  $g^{-1}$ .*

*Les isométries du plan euclidien forment un groupe (l'élément neutre est la transformation identité qui ne déplace aucun point), les permutations d'un jeu de cartes forment un groupe... En général, un groupe est donné comme agissant sur un ensemble, autrement dit on associe à tout élément du groupe une transformation de l'ensemble, de façon compatible avec la loi de composition. Une telle action est dite transitive si étant donné deux éléments  $x$  et  $y$  de l'ensemble,  $x$  peut être envoyé sur  $y$  par un élément de  $G$ . Enfin, lorsqu'un groupe admet en plus une structure de variété différentiable (encadré 2) compatible avec sa structure de groupe, on dit que c'est un groupe de Lie (groupe continu pour Poincaré). C'est le cas des groupes associés aux espaces symétriques.*

## VARIÉTÉS ARITHMÉTIQUES

Les espaces symétriques synthétisent les points de vues de Klein et Riemann sur la géométrie en un autre sens : de nombreuses variétés peuvent être modelées sur de tels espaces (encadré 2). Ainsi, Poincaré et Klein se rendent compte que toute surface peut être munie d'une géométrie sphérique, euclidienne ou hyperbolique ; décrivons ce que cela signifie.

Localement, un être bi-dimensionnel vivant sur une surface, c'est-à-dire une variété différentiable à deux dimensions, a l'impression de vivre sur un disque, de la même manière que nous avons longtemps cru que la terre était plate. Néanmoins, en agrandissant petit à petit son point de vue, un tel être sera peut-être amené à identifier des points du bord de son champ visuel (figure 1 pour l'exemple du tore). Tant que son champ de vision s'étend sans se recouper, on peut le représenter au choix comme un disque dans le plan euclidien, sur la sphère ou dans le plan hyperbolique. Mais dès que l'on doit identifier des points, sa forme change. Lorsque toutes les identifications sont faites, on ne peut plus représenter tel quel son champ de vision dans l'un de ces trois espaces, il faut spécifier la façon dont les points sur le bord du champ visuel vont se recoller.

Klein et Poincaré remarquent que toute surface peut-être découpée et étendue sur l'un des trois espaces modèles considérés ci-dessus et ce, de façon à ce que les

identifications permettant de reconstruire la surface soient spécifiées à l'aide d'isométries de cet espace modèle. Une telle procédure munit la surface d'une structure géométrique (encadré 2) et notamment d'une distance. Le jeu vidéo PacMan illustre à merveille ce phénomène : PacMan vit sur la surface d'une bouée, que l'on appelle un tore plat, munie de la géométrie euclidienne. La géométrie euclidienne est une géométrie modèle pour le tore. Il se pourrait que nous vivions nous-mêmes dans un espace (à trois dimensions) ressemblant au tore et pouvant être naturellement géométrisé par la géométrie euclidienne, comme l'espace de Klein représenté de l'intérieur (photo en début d'article).

Les espaces symétriques n'ont pas de « formes » intéressantes comme celle du tore. Autrement dit, la topologie (encadré 2) des espaces symétriques n'est pas riche. Il faut, comme ci-dessus, y penser comme à des espaces géométriques modèles. Au vu de ce que l'on a décrit au-dessus, il est naturel de se demander si ces géométries servent de modèles à des espaces finis et sans bords, dits *compacts* (comme la sphère, le tore ou l'une des surfaces de la figure 2, encadré 2). C'est la question que posent Clifford et Klein au début du siècle dernier.

En 1969, Borel apporte une réponse positive à la question de Clifford et Klein : tout espace symétrique est l'espace géométrique modèle d'une variété différentiable compacte. L'idée que développe (grandement !) Borel remonte à Poincaré et prend ses sources dans l'arithmétique du  $xvi^e$  siècle essentiellement développée par Fermat. Décrivons brièvement cette idée sur deux exemples.

En guise de premier exemple, revenons au tore. On l'a vu (grâce à PacMan), le tore est une surface qui peut être munie de la géométrie euclidienne. On peut le décrire autrement. Considérons le groupe  $\Gamma$  engendré par deux translations de vecteurs orthogonaux dans le plan. La vie que mène PacMan sur le tore plat est identique à la vie qu'il mènerait sur le plan euclidien tout entier, à ceci près que deux de ses positions sont considérées comme identiques si elles diffèrent d'une translation par un élément de  $\Gamma$ . On dit que le tore plat est le *quotient* du plan euclidien par le groupe  $\Gamma$ . Cela montre que le plan euclidien sert de modèle pour une surface compacte, le tore. La réponse à la question de Clifford et Klein dans le cas du plan euclidien est donc positive. Et cette réponse repose sur la construction du groupe  $\Gamma$ . Une façon de retrouver ce groupe est de remarquer que le groupe des isométries du plan euclidien contient comme sous-groupe le groupe  $\mathbb{R}^2$  de toutes les translations. L'ensemble des points à coordonnées entières de  $\mathbb{R}^2$  n'est autre que le groupe  $\Gamma$  ; on dit qu'il est obtenu par une construction arithmétique.

Considérons maintenant un deuxième exemple, le plan hyperbolique  $X$  (encadré 3). On veut montrer que l'espace  $X$  sert de modèle à une surface compacte. Comme dans l'encadré 3, soit  $q$  la forme quadratique

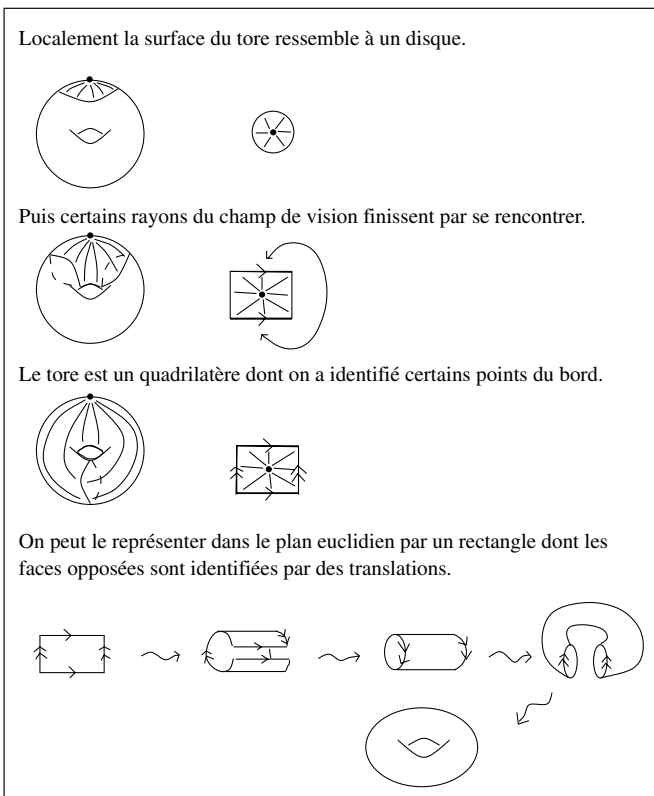


Figure 1 - Le tore euclidien.

Encadré 2

## STRUCTURES GÉOMÉTRIQUES

Fixons un ensemble  $X$  auquel on pense comme à un espace modèle. Une façon de construire de nouveaux espaces est de recoller des morceaux de  $X$  entre eux. L'espace  $X$  peut être pensé comme une réserve infinie de tissu que l'on peut découper en morceaux que l'on recolle pour former un vêtement. Pour pouvoir découper notre ensemble  $X$ , il faut définir ce que sont les morceaux de  $X$  autorisés. L'espace  $X$  équipé de cet ensemble de morceaux autorisés est appelé espace topologique et les morceaux les ouverts de  $X$ .

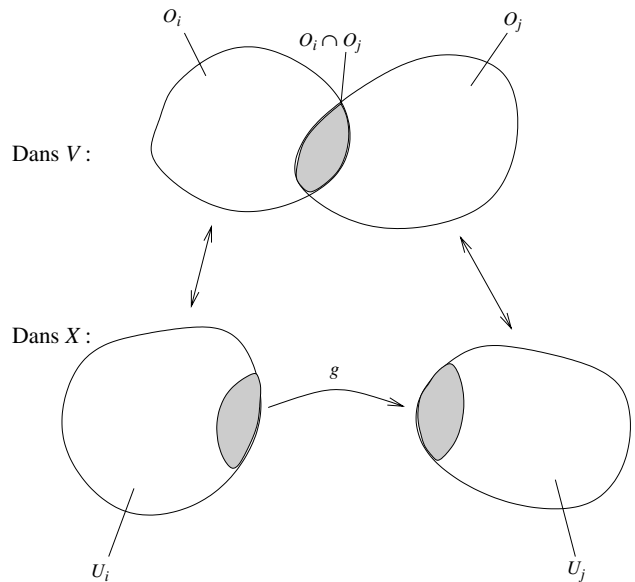
Il faut ensuite coder les façons de recoller les ouverts de  $X$  de manière à former un nouvel espace. La structure dans laquelle on code ces recollements est un groupe  $G$  agissant sur l'ensemble  $X$  (encadré 1) et transformant tout ouvert de  $X$  en un ouvert de  $X$ .

On peut alors former de nouveaux espaces modélés sur  $(X, G)$  : un espace topologique  $V$  est dit modélé sur  $(X, G)$  s'il peut s'écrire comme une réunion  $\cup_i O_i$  d'ouverts de  $V$  tels que

- chaque  $O_i$  s'identifie à un ouvert  $U_i$  de  $X$ ,
- $O_i$  est recollé à  $O_j$  par un élément  $g$  du groupe  $G$ , c'est-à-dire qu'il existe un élément  $g$  du groupe  $G$  envoyant l'image de l'intersection  $O_i \cap O_j$  dans  $U_i$  vers son image dans  $U_j$  (dessin ci-contre).

Un premier, et fondamental, exemple de structure géométrique est la notion de variété différentiable : une variété différentiable  $V$  est un espace topologique localement modélé sur l'espace euclidien  $\mathbb{R}^n$  muni de sa topologie usuelle, où les ouverts sont les réunions de boules, et du groupe des transformations bijectives de  $\mathbb{R}^n$  dans  $\mathbb{R}^n$  et partout différentiables. Une variété différentiable  $V$  est dite compacte si pour toute collection d'ouverts  $O_i$  de  $V$  dont la réunion est  $V$  tout entier, on peut trouver une sous-collection finie avec la même propriété.

Deux variétés différentiables sont considérées comme identiques s'il existe une application bijective entre elles et



différentiable. Cette structure géométrique est très souple, un ballon de rugby et un ballon de football sont considérés comme identiques. On dit de deux variétés différentiables identiques qu'elles ont la même topologie.

Une surface est une variété différentiable de dimension 2, c'est-à-dire localement modélée sur le plan euclidien.

Il existe des structures plus rigides, lorsque le groupe  $G$  est plus petit. On peut par exemple prendre pour espace modèle  $X$  un espace symétrique et pour  $G$  le groupe des isométries de  $X$ . Ce sont exactement les structures que l'on considère dans cet article. Remarquons que le ballon de rugby, qui a la même topologie que la sphère, n'est pas un espace symétrique lorsqu'on le munit de sa distance usuelle. Il n'est pas assez symétrique : les deux extrémités ne ressemblent pas métriquement aux autres points.

$q = x^2 + y^2 - 7z^2$ . L'espace symétrique  $X$  est associé au groupe des matrices réelles préservant la forme quadratique  $q$ . De manière analogue à l'exemple ci-dessus, soit alors  $\Gamma$  le groupe des matrices à coefficients entiers préservant la forme quadratique  $q$ . Le groupe  $\Gamma$  agit sur le plan hyperbolique et comme dans l'exemple du tore, on peut former le quotient du plan hyperbolique  $X$  par le groupe  $\Gamma$ . Ce quotient est une surface compacte, obtenue par une construction arithmétique et qui est naturellement modélée sur le plan hyperbolique. La réponse à la question de Clifford et Klein est donc également positive dans le cas du plan hyperbolique.

Plus généralement, Borel répond par l'affirmative à la question de Clifford et Klein pour n'importe quel espace symétrique. Pour cela, il considère certains groupes de matrices  $G$  associés aux espaces symétriques et forme les quotients de ces espaces par le sous-groupe  $G(\mathbb{Z})$  de  $G$  constitué des matrices entières. Les espaces ainsi obtenus sont des variétés différentiables compactes modélées sur les espaces symétriques respectifs. On les appelle *variétés arithmétiques*.

Au lieu du groupe de toutes les matrices à coefficients entiers  $G(\mathbb{Z})$ , on aurait pu considérer le sous-groupe

constitué de celles dont les coefficients sont congrus à ceux de la matrice identité, *modulo* un certain entier  $N \geq 1$ . On obtient ainsi différentes variétés différentiables modelées sur l'espace symétrique associé à  $G$ , que l'on appelle les *revêtements de congruence*. Ils interviendront plus loin dans le texte.

Mentionnons brièvement le lien avec l'arithmétique. Les variétés différentiables obtenues par des constructions arithmétiques comme ci-dessus sont compactes. Cela implique en particulier que les groupes  $G(\mathbb{Z})$  considérés ci-dessus sont infinis. Cela n'est pas anodin. Les premiers à avoir étudié de tels problèmes sont les arithméticiens, notamment Fermat. Étant donné la forme quadratique  $\varphi = x^2 - at^2$  où  $a$  est un entier sans facteurs carrés, le théorème de Borel, mentionné ci-dessus, implique que le groupe des matrices entières préservant  $\varphi$  est infini. Ce résultat est dû à Fermat qui démontre plus exactement que l'équation  $m^2 - an^2 = \pm 1$ , où  $m$  et  $n$  sont des entiers, a une infinité de solutions. Résultat non trivial puisque, par exemple, la plus petite solution après  $(1, 0)$  à l'équation  $m^2 - 94n^2 = \pm 1$  est  $(2\ 143\ 295, 221\ 064)$ .

Les variétés arithmétiques font l'objet de recherches intensives. Signalons notamment ces deux thèmes : les variétés à géométrie symétriques sont-elles toutes arithmétiques ? Quelle est la forme, la topologie, des variétés arithmétiques ? La réponse à la première question est essentiellement connue et est positive pour une large classe de géométries symétriques (excluant notamment la géométrie hyperbolique). Elle est l'œuvre du mathématicien russe Margulis et lui a valu la médaille Fields. Dans la suite de cet article, nous allons nous concentrer sur la deuxième question.

### UN PEU DE TOPOLOGIE

Faisons ici un petit aparté en topologie pure afin de décrire, de façon informelle, quelques outils fondamentaux dans l'étude de la forme des variétés différentiables. En effet, parallèlement aux développements des nouvelles géométries et sous l'impulsion de Riemann, Betti et Poincaré, les mathématiciens de la fin du XIX<sup>e</sup> siècle commencent à étudier les variétés du point de vue de leur forme – c'est le domaine de l'*analysis situs* maintenant appelée *topologie* (encadré 2).

Pour un topologue, un ballon de football et un ballon de rugby ont la même forme, car on peut passer de l'un à l'autre par une déformation continue. Afin de classifier les différentes formes possibles de variétés, le topologue cherche à associer à celles-ci des objets algébriques (nombres, groupes...) invariants par déformation, les *invariants topologiques*.

Les premiers invariants mis en évidence par Riemann et développés par Betti sont les *ordres de connexions* ou *nombres de Betti* :  $b_0, b_1, \dots, b_{n-1}, b_n$  où  $n$  est la dimension de la variété. Décrivons  $b_0$  et  $b_1$  dans le cas des trois surfaces de la figure 2 – la sphère, le tore et la surface de la bouée à deux places.

Le nombre  $b_0$  compte le nombre de morceaux, ou composantes connexes, de la surface. Nos trois surfaces sont d'un seul tenant, elles sont connexes. Autrement dit, le nombre  $b_0$  associé à la sphère, au tore ou à la surface de la bouée à deux places vaut 1. Il ne permet donc pas de les distinguer.

Le nombre  $b_1$  compte le nombre maximal de courbes fermées dans la surface suivant lesquelles on peut découper la surface sans augmenter le nombre de morceaux, autrement dit le nombre de courbes fermées dans la surface que l'on peut enlever sans disconnecter celle-ci. Ce nombre  $b_1$  vaut 0 dans le cas de la sphère, vaut 2 dans le cas du tore, et vaut 4 dans le cas de la surface de la bouée à deux places (figure 2). En admettant que les nombres de Betti sont effectivement invariants par déformation continue, autrement dit qu'ils sont des invariants topologiques, on obtient que le premier nombre de Betti suffit à distinguer les trois surfaces considérées du point de vue

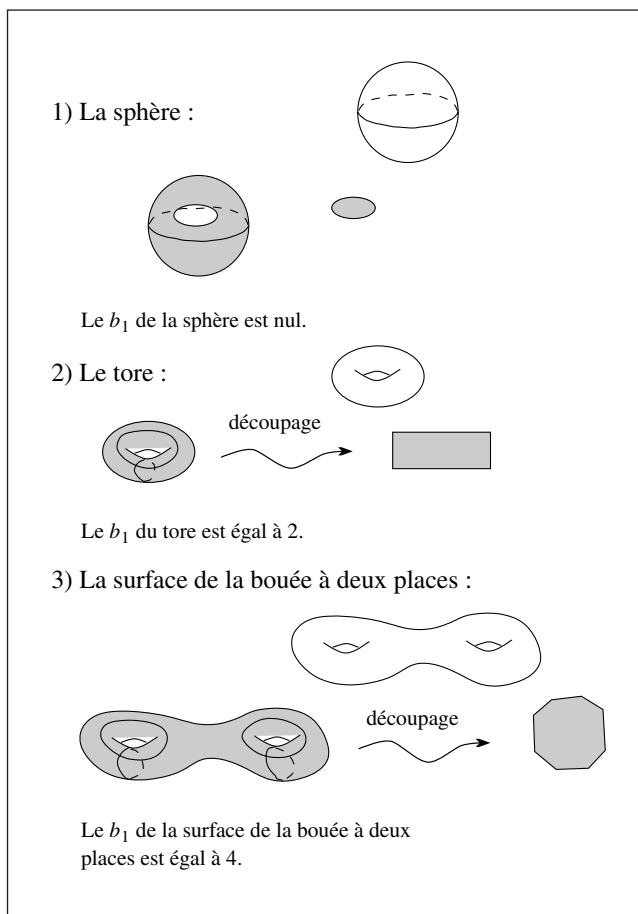
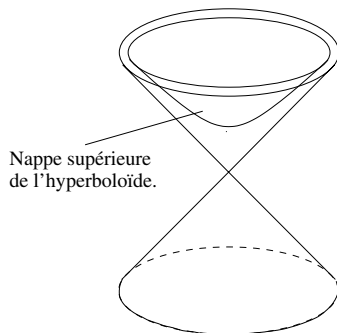


Figure 2 - Le premier nombre de Betti de quelques surfaces.

Encadré 3

## LE PLAN HYPERBOLIQUE

Dans l'espace euclidien  $\mathbb{R}^3$ , considérons la forme quadratique  $q(x, y, z) = ax^2 + by^2 - cz^2$  où  $a, b, c$  sont des nombres réels strictement positifs. L'ensemble des points  $(x, y, z)$  de l'espace euclidien qui vérifient  $q(x, y, z) = -1$  est une surface appelée l'hyperboloïde à deux nappes (figure). La nappe supérieure de cette hyperboloïde est une réalisation du plan hyperbolique. Les droites de cette géométrie sont les sous-ensembles obtenus en prenant l'intersection de la nappe supérieure de l'hyperboloïde avec des plans passant par le point  $(0, 0, 0)$ .



Le plan hyperbolique est bien une variété différentiable et on peut la munir d'une structure riemannienne, où la longueur d'un vecteur  $(dx, dy, dz)$  tangent à l'hyperboloïde est  $adx^2 + bdy^2 - cdz^2$  (qui est toujours un nombre strictement positif si le vecteur est non nul et tangent à l'hyperboloïde). Les droites du plan hyperbolique sont les plus courts chemins pour la distance induite par cette structure riemannienne. Le plan hyperbolique est un espace symétrique, le groupe associé est le groupe des matrices préservant la forme quadratique  $q$ . Remarquons que lorsque l'on change la forme quadratique (en modifiant les valeurs de  $a, b$  et  $c$ ), on change le groupe de matrices. Néanmoins, la géométrie reste la même ; en fait les groupes sont abstraitement les mêmes : ils sont isomorphes. Mais les ensembles de matrices à coefficients entiers sont différents, non isomorphes, dans chacun de ces groupes de matrices.

topologique. On ne peut donc pas passer de la surface d'un ballon à celle d'une bouée par déformation continue. Ce résultat est certes intuitif, mais il est peut-être plus surprenant que l'on puisse en donner une preuve formelle.

Plus généralement, Poincaré introduit les *groupes d'homologies*. Considérons une variété  $V$  à  $n$  dimensions ; soit maintenant  $W$  une variété à  $p$  dimensions ( $p \leq n$ ) faisant partie de  $V$  et avec un bord (voir par exemple figure 3). Supposons que le bord de  $W$  se compose de  $l$  variétés à  $p - 1$  dimensions :

$$v_1, v_2, \dots, v_l.$$

Poincaré exprime ce fait par la notation

$$v_1 + v_2 + \dots + v_l \sim 0$$

qui se lit « analogue à 0 », ou *homologue à 0*.

Plus généralement la notation

$$k_1 v_1 + k_2 v_2 \sim k_3 v_3 + k_4 v_4,$$

où les  $k_i$  sont des entiers et les  $v_i$  des variétés à  $p - 1$  dimensions, exprime qu'il existe une variété  $W$  à  $p$  dimen-

sions faisant partie de  $V$  et dont le bord se compose de  $k_1$  variétés peu différentes de  $v_1$  (c'est-à-dire obtenues par déformation continue de  $v_1$  dans  $V$ ), de  $k_2$  variétés peu différentes de  $v_2$ , de  $k_3$  variétés peu différentes de la variété opposée (au sens de l'orientation) à  $v_3$  et de  $k_4$  variétés peu différentes de la variété opposée à  $v_4$ .

Poincaré appelle les relations de cette forme des *homologies*. Les homologies peuvent se combiner comme des équations ordinaires et permettent ainsi d'associer un groupe pour chaque dimension  $p$ , dont Poincaré prouve qu'il est invariant par déformation continue. Le développement et la formalisation de cette théorie a énormément occupé les mathématiciens jusqu'aux années 1950.

On dit que les variétés

$$v_1, v_2, \dots, v_l,$$

d'un même nombre de dimensions et faisant partie de  $V$ , sont *linéairement indépendantes*, si elles ne sont liées par aucune homologie à coefficients entiers.

S'il existe  $b_l$  variétés fermées à  $l$  dimensions faisant partie de  $V$  et linéairement indépendantes et s'il n'existe que  $b_l$ , on dit que l'ordre de connexion de  $V$  par

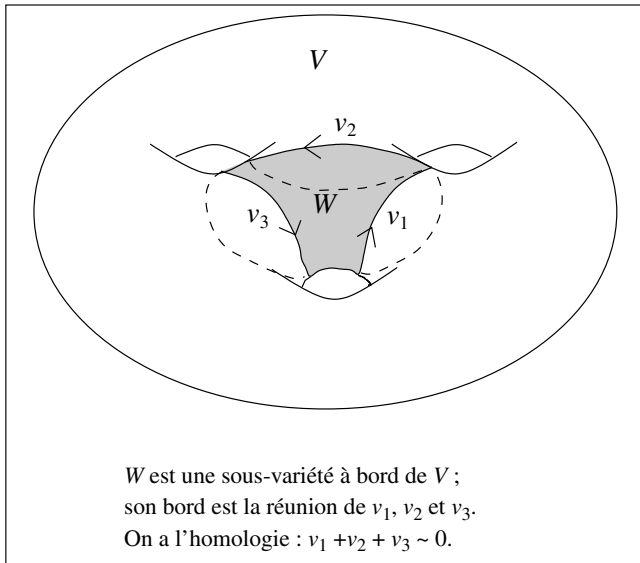


Figure 3 - Une homologie.

rapport aux variétés à  $l$  dimensions est égal à  $b_l$ , ou que  $b_l$  est le  $l$ -ième nombre de Betti de  $V$ .

Comme l'a remarqué Poincaré, ni les nombres de Betti, ni les groupes d'homologie définis ci-dessus ne permettent de classer toutes les variétés : il existe deux variétés de même dimension qui ont les mêmes groupes d'homologie bien que l'on ne puisse pas passer de l'une à l'autre par déformation continue. Néanmoins, ce sont des invariants fondamentaux et la première étape pour comprendre la forme d'une variété consiste à comprendre ses homologies.

### HOMOLOGIES DES VARIÉTÉS ARITHMÉTIQUES

Afin de comprendre la topologie (la forme) des variétés arithmétiques, on cherche à comprendre leurs homologies.

Par exemple, une question non encore totalement résolue est de savoir si, étant donnée une variété arithmétique  $V$  de dimension  $n$ , il existe ou non un revêtement de congruence contenant une sous-variété  $v$  à  $n - 1$  dimensions qui ne soit pas homologue à 0.

A travers plusieurs travaux récents, il apparaît que dans de nombreux cas, les homologies d'une variété arithmétique, ou plutôt de l'ensemble de ses revêtements de congruence, peuvent être « déduites » des homologies de certaines de ses sous-variétés.

Commençons par une description informelle de cette « philosophie ». Soient  $X$  et  $Y$  deux espaces symétriques tels que  $Y$  soit réalisé comme sous-espace de  $X$ . Considérons  $H$  et  $G$ , deux groupes de matrices respectivement associés aux espaces symétriques respectifs  $Y$  et  $X$ . Les groupes  $H$  et  $G$  sont donc des groupes de matrices réelles agissant transitivement et par transformations isométriques respectivement sur les espaces  $Y$  et  $X$ . On demande de plus que les groupes  $H$  et  $G$  vérifient que :

1.  $H$  et  $G$  sont tous les deux des groupes auxquels Borel nous a appris à associer des variétés arithmétiques ;
2.  $H$  est contenu, comme groupe, dans  $G$  ; le groupe  $H$  agit alors par isométries sur  $X$  en préservant  $Y$ .

Notons  $\Lambda = H(\mathbb{Z})$  et  $\Gamma = G(\mathbb{Z})$  les sous-groupes respectifs de  $H$  et  $G$  constitués des matrices entières. Les quotients  $W$  et  $V$  des espaces  $Y$  et  $X$  respectivement par les groupes  $\Lambda$  et  $\Gamma$  sont des variétés arithmétiques associées à  $H$  et  $G$ . De plus, la variété  $W$  fait partie de la variété  $V$  ; on dit que c'est une *sous-variété arithmétique*.

On s'attend, et cela a été effectivement démontré dans certains cas, à ce que les variétés de suffisamment grande dimension contenues dans  $W$ , et qui sont donc aussi contenues dans  $V$ , n'aient pas plus de relations d'homologies dans un revêtement de congruence de  $V$  que dans  $W$ . Dualement, on s'attend également à ce que toute variété de suffisamment petite dimension et contenue dans  $V$  soit homologue à une variété contenue dans une variété  $W$  obtenue comme ci-dessus.

De telles propriétés sont très restrictives au niveau topologique : les groupes d'homologies des variétés arithmétiques devraient être presque entièrement compris à l'aide des groupes d'homologies de variétés arithmétiques plus petites et, on l'espère, plus simples.

Concluons ce texte par un véritable énoncé dans la lignée de cette philosophie, récemment obtenu dans cette généralité.

**Théorème.** Soit  $V$  une variété arithmétique de dimension  $n$  contenant des sous-variétés arithmétiques de dimension  $k < n$ . Supposons que  $V$  contienne une sous-variété  $C$  de dimension  $n - 1$  et non homologue à zéro dans  $V$ . Alors, il existe une sous-variété arithmétique  $W$  de  $V$  de dimension  $k$  et telle que l'intersection de  $W$  et  $C$  soit une sous-variété de  $W$  de dimension  $k - 1$  et non homologue à zéro dans  $W$ .

# Probabilités libres et matrices aléatoires

**Motivé par des problèmes de classification d'algèbres d'opérateurs, Voiculescu a inventé des outils de nature probabiliste qui se sont révélés très utiles pour comprendre la structure des matrices aléatoires de grande taille. Ainsi, en utilisant la théorie de Voiculescu, on peut avec une bonne précision et une faible chance de se tromper, prédire la forme du spectre de la somme de deux grandes matrices hermitiennes, en connaissant seulement le spectre de chacune d'elles.**

Diagonaliser des matrices hermitiennes est une activité courante aussi bien en mathématiques qu'en physique. Il arrive souvent que la matrice à diagonaliser se présente sous la forme d'une somme de deux matrices hermitiennes  $A$  et  $B$  dont on connaît les spectres. L'ensemble de tous les spectres possibles pour  $A + B$  peut être déterminé explicitement en fonction de ceux de  $A$  et  $B$ . Par exemple, il est facile de voir que si  $A$  et  $B$  sont des matrices  $2 \times 2$  et si, en écrivant les valeurs propres dans l'ordre décroissant, on a  $Sp(A) = \{\lambda_1, \lambda_2\}$  et  $Sp(B) = \{\mu_1, \mu_2\}$ , alors on a

$$Sp(A + B) = \{\nu_1, \nu_2\}$$

où  $\nu_1$  et  $\nu_2$  vérifient

$$\begin{aligned} \nu_1 + \nu_2 &= \lambda_1 + \lambda_2 + \mu_1 + \mu_2 \\ |(\lambda_1 - \lambda_2) - (\mu_1 - \mu_2)| &\leq \nu_1 - \nu_2 \\ \nu_1 - \nu_2 &\leq \lambda_1 - \lambda_2 + \mu_1 - \mu_2. \end{aligned}$$

De plus, tous les couples  $(\nu_1, \nu_2)$  satisfaisant ces conditions peuvent être réalisés en choisissant convenablement les vecteurs propres des matrices  $A$  et  $B$ . Pour des matrices de taille arbitraire, un ensemble complet d'inégalités caractérisant l'ensemble de tous les spectres possibles a été obtenu récemment par Klyachko, résolvant ainsi un problème qui remonte à Weyl. Toutefois pour des matrices de grande taille, lorsque l'on fixe les spectres des matrices  $A$  et  $B$  et que l'on choisit leurs vecteurs propres au hasard, on s'aperçoit que parmi tous les spectres possibles pour  $A + B$ , seul un tout petit sous-ensemble est réalisé avec une probabilité proche de 1. Cette proposition est illustrée par un exemple concret dans l'encadré 1. Des arguments très généraux, regroupés sous le nom générique de « concentration de la mesure » permettent de prédire un tel phénomène. En effet, c'est un principe bien établi que dans des espaces de grandes dimensions (ici

les groupes de matrices unitaires de grande taille), les fonctions « raisonnables » tendent à être concentrées autour de leur moyenne, au sens de la mesure. Par exemple, si l'on considère la mesure de probabilités invariante par rotations sur une sphère de rayon 1, alors pour tout  $\epsilon > 0$  la probabilité pour que la première coordonnée satisfasse  $|x_1| \leq \epsilon$  tend vers 1 lorsque la dimension de la sphère tend vers l'infini. On s'attend donc à ce que le comportement moyen du spectre de la somme  $A + B$  soit aussi le comportement dominant, c'est-à-dire celui qui apparaîtra avec une grande probabilité. Toutefois, la généralité de ces principes ne nous permet pas d'en déduire cette valeur moyenne, qui dépend de la nature exacte des espaces et des fonctions que l'on considère. C'est ici qu'intervient la théorie des probabilités libres de Voiculescu. Introduite à l'origine pour résoudre des problèmes de classification d'algèbres d'opérateurs, il est apparu que cette théorie fournit le cadre algébrique adéquat pour modéliser le comportement le plus probable d'une famille de matrices dont les vecteurs propres ont été choisis au hasard, et permet de faire de nombreux calculs. Ces relations profondes avec les matrices aléatoires ont fait des probabilités libres un outil extrêmement puissant, qui a permis de résoudre de nombreux problèmes ouverts sur les algèbres d'opérateurs. Je n'aborderai pas ces questions ici, faute de place, mais je vais décrire le formalisme algébrique dans la section suivante, en explicitant la notion de liberté, puis j'expliquerai comment cela s'applique aux matrices aléatoires de grande taille.

## LA LIBERTÉ

On considère une algèbre complexe  $A$ , avec une unité 1 et une forme linéaire  $\tau : A \rightarrow \mathbb{C}$ , telle que  $\tau(1) = 1$ . Bien que les exemples intéressants pour la théorie soient hautement non commutatifs, il est utile pour l'intuition de se représenter les éléments de l'algèbre  $A$  comme des variables aléatoires et l'application  $\tau$  comme étant l'espérance. En particulier, si  $a \in A$ , on appellera moments de  $a$  les nombres  $\tau(a^n)$ ;  $n \geq 1$ . On a coutume d'appeler un tel couple  $(A, \tau)$  un *espace de probabilités non commutatif*. La définition de base de la théorie est la suivant-

---

– Philippe Biane, Département de mathématiques et applications – UMR 8553 CNRS – École normale supérieure, 45 rue d'Ulm, 75230 Paris cedex 05.  
philippe.biane@ens.fr



**Encadré 1**

**SOMME DE DEUX PROJECTEURS**

On tire au hasard, et indépendamment, deux projecteurs orthogonaux  $\Pi_1$  et  $\Pi_2$  de rang  $N$  dans un espace complexe de dimension  $2N$ , sous la forme  $\Pi_i = U_i D U_i^*$  où  $D$  est la matrice diagonale dont les  $N$  premiers éléments diagonaux valent 1 et les autres 0, et  $U_i$  est une matrice unitaire, choisie selon la mesure de Haar sur le groupe unitaire  $U(2N)$ . Tirer une matrice unitaire selon la mesure de Haar est très facile : on commence par tirer le premier vecteur colonne uniformément parmi tous les vecteurs de norme 1, puis on choisit le deuxième vecteur colonne uniformément parmi les vecteurs de norme 1 orthogonaux au premier, et ainsi de suite. Un moyen simple de réaliser cela consiste à choisir une matrice  $2N \times 2N$  à coefficients indépendants avec des lois gaussiennes complexes standard, puis à appliquer le procédé de Gramm-Schmidt à ses vecteurs colonnes.

La figure représente l'histogramme obtenu à partir du spectre d'une matrice  $\Pi_1 + \Pi_2$  choisie comme ci-dessus, avec  $N = 400$ . Avec deux projections de rang 400 on peut obtenir des histogrammes très différents, par exemple si  $\Pi_1 = I - \Pi_2$  alors toutes les valeurs propres valent 1, alors que si  $\Pi_1 = \Pi_2$  la moitié vaut 2 et l'autre moitié vaut 0, mais on observe que pour  $N$  grand, avec une probabilité presque égale à 1, cet histogramme reste dans le voisinage d'une certaine courbe, que la théorie des probabilités libres permet de calculer explicitement.

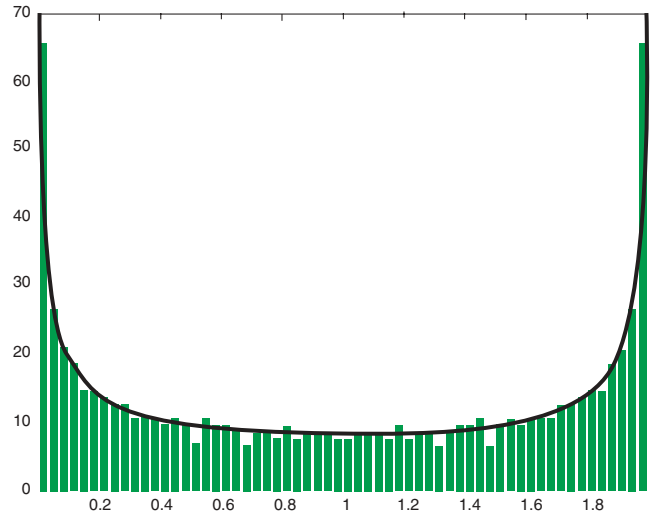


Figure - Histogramme du spectre de  $\Pi_1 + \Pi_2$ .

Dans le cas de notre figure, cette courbe est le graphe de la fonction  $y = \frac{80}{3\pi\sqrt{x(2-x)}}$ .

te, qui est un analogue non commutatif de la notion d'indépendance en théorie des probabilités.

**Définition.** Une famille  $(A_i; i \in I)$  de sous-algèbres unitales de  $A$ , est dite libre dans  $(A, \tau)$  si pour tout choix d'éléments  $a_1, \dots, a_n \in \cup_{i \in I} A_i$ , vérifiant  $\tau(a_1) = \dots = \tau(a_n) = 0$  et  $a_j \in A_{i_j}$  avec  $i_1 \neq i_2 \neq \dots \neq i_n$ , on a  $\tau(a_1 a_2 \dots a_n) = 0$ .

Dans cette définition, les indices voisins sont supposés distincts, mais on autorise par exemple  $i_1 = i_3$ . La notion de liberté incorpore à la fois le concept d'indépendance des probabilités classiques et celui d'indépendance algébrique, même si cela ne saute pas aux yeux en lisant la définition, qui peut paraître compliquée. Un petit calcul va permettre de se familiariser avec la liberté. On considère  $(A_1, A_2)$  une famille libre dans  $(A, \tau)$ , et  $a_1 \in A_1, a_2 \in A_2$ . Si on pose  $\bar{a}_i = a_i - \tau(a_i)1, i = 1, 2$  alors le calcul classique de la covariance montre que

$$\tau(\bar{a}_1 \bar{a}_2) = \tau(a_1 a_2) - \tau(a_1)\tau(a_2)$$

et l'hypothèse de liberté entraîne que  $\tau(\bar{a}_1 \bar{a}_2) = 0$ . On en déduit que

$$\tau(a_1 a_2) = \tau(a_1)\tau(a_2). \tag{1}$$

En fait, ce calcul se généralise et l'on montre que si  $a = a_1 \dots a_n$  est un « mot », produit de termes  $a_j \in A_{i_j}$  où  $(A_i; i \in I)$  est une famille libre dans  $(A, \tau)$ , alors  $\tau(a)$  peut s'exprimer comme un polynôme en les quantités de la forme  $\tau(a_{j_1} \dots a_{j_k})$  où tous les termes du produit  $a_{j_1}, \dots, a_{j_k}$ , appartiennent à une même sous-algèbre  $A_i$ . Par exemple, en reprenant les notations ci-dessus, on peut vérifier que

$$\begin{aligned} \tau(a_1 a_2 a_1 a_2) &= \tau(a_1^2) \tau(a_2)^2 \\ &+ \tau(a_1)^2 \tau(a_2^2) - \tau(a_1)^2 \tau(a_2)^2. \end{aligned} \tag{2}$$

On en déduit en particulier que si  $(A_i; i \in I)$  est une famille libre, alors la restriction de  $\tau$  à la sous-algèbre engendrée par la famille  $(A_i; i \in I)$  est entièrement déterminée par les restrictions de  $\tau$  à chacune des sous-algèbres  $A_i$ . Cette propriété est analogue à celle de l'indépendance des variables aléatoires en probabilités classiques ; on sait bien en effet que si l'on dispose d'une famille de variables aléatoires indépendantes et que l'on connaît la loi de chacune d'elles, alors on peut calculer la loi jointe de cette famille de variables aléatoires. Enfin,

on peut vérifier que la notion de liberté est non vide ; si l'on se donne une famille d'espaces de probabilités non commutatifs  $(A_i, \tau_i); i \in I$ , alors on peut toujours, au moyen d'une construction de produit libre réduit, trouver un espace de probabilités non commutatif  $(A, \tau)$  et des morphismes d'algèbres  $\iota_i : A_i \rightarrow A$ , injectifs, préservant l'unité et vérifiant  $\tau_i = \tau \circ \iota_i$ , tels que les sous-algèbres  $(A_i; i \in I)$  forment une famille libre dans  $(A, \tau)$ .

### LIBERTÉ ASYMPTOTIQUE DES MATRICES ALÉATOIRES

Voyons maintenant comment la notion de liberté permet de modéliser le comportement des grandes matrices aléatoires. Commençons par rappeler que, d'après le théorème spectral, une matrice hermitienne  $M$  de taille  $N \times N$  est déterminée, à une conjugaison par une matrice unitaire près, par son spectre (avec la multiplicité de chaque valeur propre), c'est-à-dire un ensemble de  $N$  nombres réels. Des résultats classiques sur les fonctions symétriques montrent que la donnée du spectre de la matrice  $M$  est elle-même équivalente à celle de la suite de nombres  $\frac{1}{N} Tr(M^n); n \geq 1$ , (en fait il suffit de connaître seulement les  $N$  premiers termes de cette suite). Cette suite de nombres est aussi la suite des moments de la mesure  $\frac{1}{N} \sum_j \delta_{\lambda_j}$  où  $\lambda_1, \dots, \lambda_N$  désigne le spectre de  $M$ , les valeurs propres étant comptées avec leur multiplicité. Il est commode de désigner par  $tr = \frac{1}{N} Tr$  la trace normalisée sur l'espace de matrices de taille  $N \times N$ , ce que je ferai dans la suite. Si l'on considère plusieurs matrices  $M_1, \dots, M_m$ , la donnée du spectre de chacune d'elles ne suffit pas à déterminer leurs positions relatives dans l'espace de toutes les matrices hermitiennes. Néanmoins, une construction classique dans la théorie des algèbres d'opérateurs, la construction de Gelfand-Naimark-Segal (GNS) montre que si l'on connaît les nombres  $tr(M_{i_1} \dots M_{i_k})$  où  $k$  parcourt les entiers positifs et les indices  $i_1, \dots, i_k$  prennent des valeurs arbitraires dans  $\{1, \dots, m\}$ , alors on peut retrouver les matrices  $M_i$  à une conjugaison unitaire globale près  $M_i \mapsto U M_i U^*$  (c'est-à-dire que  $U$  ne dépend pas de  $i$ ). Il est facile de voir que la connaissance de ces nombres permet de retrouver le spectre de n'importe quel polynôme en les matrices  $M_1, \dots, M_m$ . Supposons maintenant que les spectres des matrices  $M_1, M_2, \dots, M_m$  sont fixés et inclus dans  $[-1, 1]$  pour fixer les idées (on peut toujours tout multiplier par une constante pour s'y ramener), mais que leurs vecteurs propres sont choisis au hasard. Autrement dit, les matrices ont la forme  $M_i = U_i D_i U_i^*$  où les matrices  $D_i$  sont diagonales et les matrices  $U_i$  sont des matrices unitaires choisies au hasard, indépendamment, et avec la mesure de Haar sur le groupe unitaire  $U(N)$ . On se donne alors un espace de probabilités non commutatif

$(A, \tau)$  et des éléments  $a_1, \dots, a_m \in A$ , tels que les sous-algèbres  $A_i; i \in I$  (où  $A_i$  désigne la sous-algèbre unitaire engendrée par  $a_i$ ) forment une famille libre. Comme on l'a vu, l'hypothèse de liberté entraîne que la quantité  $\tau(a_{i_1} \dots a_{i_k})$  peut s'exprimer comme un polynôme en les moments  $\tau(a_i^n)$ . Le résultat fondamental de Voiculescu est que la valeur de  $tr(M_{i_1} \dots M_{i_k})$  est proche de  $\tau(a_{i_1} \dots a_{i_k})$  avec une probabilité qui tend vers 1 lorsque  $N$  tend vers l'infini. Plus précisément, pour tout choix d'un réel  $\varepsilon > 0$ , et d'un multiindice  $(i_1, \dots, i_k)$ , il existe une suite  $C_N$ , qui tend vers zéro lorsque  $N$  tend vers l'infini et telle que, pour tout  $N$ , la probabilité pour que

$$|tr(M_{i_1} \dots M_{i_k}) - \tau(a_{i_1} \dots a_{i_k})|$$

soit plus grand que  $\varepsilon$  est majorée par  $C_N$ , cette inégalité étant vérifiée pour tout choix des spectres de  $M_1, \dots, M_m$  dans  $[-1, 1]$ .

En utilisant ce résultat on peut prédire, avec une bonne précision et une probabilité proche de 1, la valeur d'une quantité de la forme  $tr(M_{i_1} \dots M_{i_k})$ , en connaissant seulement les spectres de  $M_1, \dots, M_m$ . Par exemple, en reprenant la formule (1) on voit que pour « la plupart » des couples de matrices de grande taille  $M_1, M_2$ , on a

$$tr(M_1 M_2) \sim tr(M_1) tr(M_2)$$

ou encore, en utilisant (2)

$$\begin{aligned} tr(M_1 M_2 M_1 M_2) &\sim \\ tr(M_1^2) tr(M_2)^2 + tr(M_1)^2 tr(M_2^2) &- \\ -tr(M_1)^2 tr(M_2)^2. \end{aligned}$$

De même, on peut calculer grâce à ce théorème le comportement asymptotique des moments  $tr((M_1 + M_2)^n); n \geq 1$  de la somme de deux matrices, en termes des deux suites de moments  $tr(M_1^n); n \geq 1$  et  $tr(M_2^n); n \geq 1$ . La connaissance d'un nombre fini de moments ne permet pas de retrouver tout le spectre (n'oublions pas que  $N \rightarrow \infty$ ), mais elle permet d'avoir une bonne approximation de la mesure empirique de ce spectre. C'est ce qui permet de tracer la courbe de l'encadré 1. Les calculs algébriques se font au niveau des algèbres libres, sans référence aux matrices aléatoires. Il reste à expliquer comment faire ces calculs de façon économique, ce qui est loin d'être évident. C'est ce que je vais faire dans la section suivante, en décrivant la méthode combinatoire de Speicher.

### COMBINATOIRE DE LA LIBERTÉ

La notion combinatoire adéquate pour faire des calculs en probabilités libres est celle de partition non croisée. Une partition de l'ensemble  $\{1, 2, \dots, n\}$  est dite croisée s'il existe deux classes distinctes  $C$  et  $D$  de la partition et quatre éléments  $i, j, k, l \in \{1, 2, \dots, n\}$  tels

que  $i < j < k < l$ , on a  $i, k \in C$  et  $j, l \in D$ . Elle est dite non croisée dans le cas contraire. L'ensemble des partitions non croisées de  $\{1, 2, \dots, n\}$  est noté  $NC(n)$ . C'est

une structure combinatoire très riche, qui mérite d'être étudiée pour elle-même (voir l'encadré 2 pour plus d'informations sur cette notion).

**Encadré 2**

**LES PARTITIONS NON CROISÉES**

On considère une partition de l'ensemble  $\{1, \dots, n\}$ . Il est commode de placer les  $n$  points sur un cercle et de tracer, pour chaque classe de la partition, le polygone convexe dont les sommets sont les points dans la classe. La partition est non croisée si et seulement si ces polygones ne s'intersectent pas.

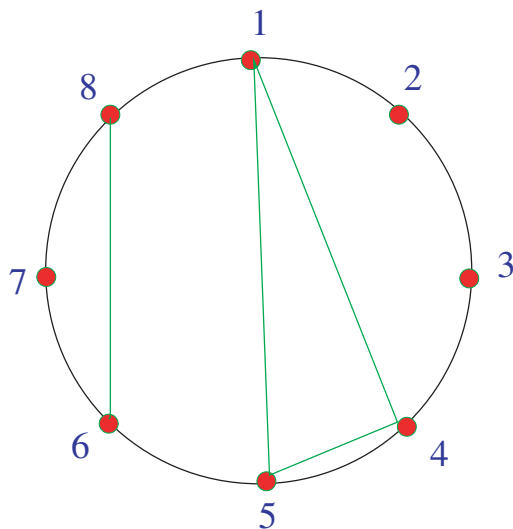


Figure 1 - Une partition non croisée.

La figure ci-dessus montre la partition non croisée  $\{1, 4, 5\} \cup \{2\} \cup \{3\} \cup \{6, 8\} \cup \{7\}$ . Le nombre de partitions non croisées de  $\{1, \dots, n\}$  est le nombre de Catalan  $\frac{(2n-2)!}{n!(n-1)!}$ . La relation « est moins fine que » est une relation d'ordre qui fait de l'ensemble des partitions non croisées un treillis (tout sous-ensemble admet un plus petit majorant et un plus grand minorant). Les partitions non croisées interviennent dans l'étude du groupe symétrique ; en effet on peut associer à chaque partition non croisée la permutation dont les cycles sont obtenus en parcourant chaque polygone dans le sens des aiguilles d'une montre. On obtient ainsi un sous-ensemble du groupe des permutations de  $\{1, \dots, n\}$  qui admet une caractérisation géométrique simple. On munit le groupe symétrique de la structure de graphe de Cayley induite par l'ensemble de générateurs formé de toutes les transpositions. Autrement dit, deux permutations  $\sigma_1$  et  $\sigma_2$  sont les sommets d'une arête de ce graphe si et seulement si  $\sigma_1\sigma_2^{-1}$  est une transposition. Les permutations obtenues à partir d'une partition non croisée sont alors celles qui se situent sur une géodésique, c'est-à-dire un

chemin de longueur minimale reliant l'identité à la permutation circulaire  $c = (12 \dots n)$  dans le graphe de Cayley. On peut exprimer cette condition à l'aide de la fonction de longueur sur le groupe symétrique :  $|\sigma|$  est le plus petit nombre  $k$  tel que  $\sigma$  peut s'écrire comme le produit de  $k$  transpositions. Une permutation  $\sigma$  provient d'une partition non croisée si et seulement si on a  $|\sigma| + |\sigma^{-1}| = |c|$ . Ce plongement de  $NC(n)$  dans le groupe symétrique  $S_n$  permet de montrer que le treillis des partitions non croisées est autodual ; en effet l'application  $\sigma \mapsto \sigma^{-1}c$  de  $S_n$  dans lui-même préserve  $NC(n)$  et induit un antiautomorphisme de la structure d'ordre. Cette propriété de  $NC(n)$  n'est pas partagée par le treillis de toutes les partitions, ce qui fait que par certains côtés la théorie des probabilités libres possède plus de symétries que la théorie classique.

La figure 2 montre le treillis des partitions non croisées de  $\{1, 2, 3, 4\}$  (chacune étant identifiée avec sa permutation image).

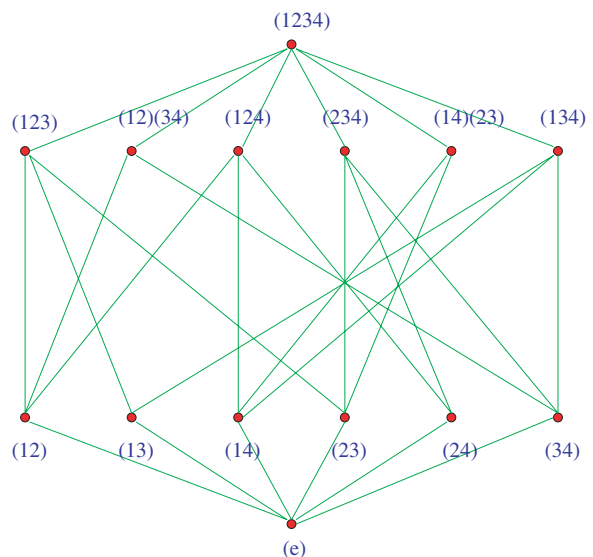


Figure 2 -  $NC(4)$ .

L'élément minimal est l'identité, l'élément maximal est la permutation circulaire (1234). La relation d'ordre est indiquée par les arêtes du graphe, qui sont aussi les arêtes du graphe de Cayley de  $S_4$ , restreint aux éléments se trouvant sur une géodésique reliant la permutation identité au cycle (1234).

Speicher s'est inspiré de l'approche algébrique de l'indépendance en théorie des probabilités due à Rota, qui utilise le treillis des partitions d'un ensemble fini pour définir les cumulants d'une famille de variables aléatoires. C'est ainsi qu'il a défini des « cumulants non croisés » de la façon suivante. Étant donné un espace de probabilités non commutatif  $(A, \tau)$ , les cumulants non croisés sont une famille  $R^{(n)}$ ;  $n \geq 1$  de formes multilinéaires sur  $A$ , définies de manière implicite ( $R^{(n)}$  étant une forme  $n$ -linéaire) par les équations

$$\tau(a_1 \dots a_n) = \sum_{\pi \in NC(n)} R_{\pi}(a_1, \dots, a_n).$$

Dans cette formule, pour chaque partition non croisée  $\pi = \cup_i A_i$ , avec  $p_i = \text{cardinal}(A_i)$ , on a

$$R_{\pi}(a_1, \dots, a_n) = \prod_i R^{(p_i)}(a_{j_1}, \dots, a_{j_{p_i}})$$

où  $A_i = \{a_{j_1}, \dots, a_{j_{p_i}}\}$ . Par exemple, pour  $n = 3$  il y a cinq termes, qui correspondent respectivement aux partitions  $\{1, 2, 3\}$ ,  $\{1\} \cup \{2, 3\}$ ,  $\{1, 3\} \cup \{2\}$ ,  $\{1, 2\} \cup \{3\}$  et  $\{1\} \cup \{2\} \cup \{3\}$ .

$$\begin{aligned} \tau(a_1 a_2 a_3) &= R_3(a_1, a_2, a_3) + R_1(a_1)R_2(a_2, a_3) \\ &\quad + R_2(a_1, a_3)R_1(a_2) + R_2(a_1, a_2)R_1(a_3) \\ &\quad + R_1(a_1)R_1(a_2)R_1(a_3) \end{aligned}$$

En général,  $\tau(a_1 \dots a_n)$  est égal à la somme de  $R^{(n)}(a_1, \dots, a_n)$  et de termes qui font intervenir les  $R^{(k)}$  avec  $k < n$ , ce qui fait que les  $R^{(n)}$  sont bien définis par récurrence sur  $n$ . Par exemple on a

$$\begin{aligned} R^{(1)}(a) &= \tau(a) \\ R^{(2)}(a_1, a_2) &= \tau(a_1 a_2) - \tau(a_1)\tau(a_2) \\ R^{(3)}(a_1, a_2, a_3) &= \tau(a_1 a_2 a_3) - \tau(a_1)\tau(a_2 a_3) \\ &\quad - \tau(a_2)\tau(a_1 a_3) - \tau(a_3)\tau(a_1 a_2) \\ &\quad + 2\tau(a_1)\tau(a_2)\tau(a_3). \end{aligned}$$

L'intérêt des cumulants non croisés provient du résultat suivant. Soit  $(A_i; i \in I)$  une famille libre dans un espace de probabilités non commutatif  $(A, \tau)$ , alors pour tout choix d'éléments  $a_1, \dots, a_n \in \cup_{i \in I} A_i$  avec  $a_j \in A_{i_j}$ , on a

$$R^{(n)}(a_1, \dots, a_n) = 0$$

dès qu'il existe deux  $i_k$  et  $i_l$  distincts.

Pour illustrer la puissance de ce résultat, considérons le cas de deux éléments  $a_1$  et  $a_2$  appartenant à des sous-algèbres libres  $A_1$  et  $A_2$ , et calculons

$$R^{(n)}(a_1 + a_2, a_1 + a_2, \dots, a_1 + a_2).$$

Si l'on développe par multilinéarité, alors le résultat ci-dessus entraîne que les termes contenant à la fois  $a_1$  et  $a_2$  sont nuls, par conséquent on a

$$\begin{aligned} R^{(n)}(a_1 + a_2, \dots, a_1 + a_2) &= R^{(n)}(a_1, \dots, a_1) \\ &\quad + R^{(n)}(a_2, \dots, a_2). \end{aligned}$$

Comme les moments  $\tau((a_1 + a_2)^n)$  peuvent se retrouver à partir des cumulants  $R^{(n)}(a_1 + a_2, \dots, a_1 + a_2)$ , on en déduit une expression explicite des moments de  $a_1 + a_2$ . On peut mettre ce calcul sous une forme plus explicite en introduisant la fonction génératrice des moments

$$G_a(z) = \frac{1}{z} + \sum_{k=1}^{\infty} \frac{\tau(a^k)}{z^{k+1}}.$$

On peut inverser cette série, au sens de la composition des séries formelles. Son inverse se met sous la forme

$$K_a(z) = \frac{1}{z} + \sum_{k=1}^{\infty} R_k(a)z^{k-1}$$

où le coefficient  $R_k(a)$  s'exprime polynomialement en terme des moments  $\tau(a^j)$  avec  $j \leq k$ , et on a

$$R_n(a) = R^{(n)}(a, \dots, a).$$

Pour calculer les moments de  $a_1 + a_2$  on doit donc :

- i) calculer les fonctions génératrices  $G_{a_1}$  et  $G_{a_2}$ ,
- ii) inverser ces fonctions pour trouver  $K_{a_1}$  et  $K_{a_2}$ ,
- iii) calculer  $K_{a_1+a_2}(z) = K_{a_1}(z) + K_{a_2}(z) - \frac{1}{z}$ ,
- iv) calculer  $G_{a_1+a_2}$  en inversant  $K_{a_1+a_2}$ ,
- v) extraire les coefficients du développement de  $G_{a_1+a_2}$ .

Reprenons l'exemple de l'encadré 1. Pour une projection orthogonale de rang  $N$  dans un espace de dimension  $2N$  on a  $\text{tr}(\Pi^k) = \frac{1}{2}$  pour  $k \geq 1$  d'où

$$G_{a_i}(z) = \frac{2z - 1}{2z(z - 1)}.$$

On en déduit

$$K_{a_i}(z) = \frac{z + 1 + \sqrt{z^2 + 1}}{2z}.$$

La série génératrice des moments de la somme de deux variables libres  $a_1$  et  $a_2$  ayant les moments de  $\Pi_1$  et  $\Pi_2$  est donc la fonction inverse de

$$K_{a_2}(z) + K_{a_2}(z) - \frac{1}{z} = 1 + \frac{\sqrt{z^2 + 1}}{z}$$

soit

$$G_{a_1+a_2}(z) = \frac{1}{\sqrt{z(z-2)}}.$$

On en déduit que les moments  $\tau((a_1 + a_2)^k)$  sont les moments de la mesure de probabilités sur  $[0, 2]$  de densité  $\frac{1}{\pi\sqrt{x(2-x)}}$ , ce qui a permis de tracer la courbe dans la figure 1.

Bien d'autres calculs sont possibles : on peut calculer par exemple de façon compacte les moments d'un produit  $\tau((a_1 a_2)^n)$  en terme des moments de  $a_1$  et  $a_2$ . Cela permet de prédire, pour des matrices unitaires aléatoires  $U_1$  et  $U_2$ , de grandes tailles, le spectre de leur produit en fonction du spectre de chacune d'elles. On peut encore traiter par ces méthodes le cas du spectre de  $A^{1/2} B A^{1/2}$  où  $A$  et  $B$  sont hermitiennes positives, ou encore celui du commutateur  $[X, Y] = XY - YX$  de deux matrices hermitiennes.

#### POUR EN SAVOIR PLUS

**Biane (P.)**, Free probability for probabilists, *math.PR/9809193*, 16 p., 1998.

**Biane (P.)**, Entropie libre et algèbres d'opérateurs, *Séminaire Bourbaki*, exposé 889, juin 2001.

**Fulton (W.)**, Eigenvalues of sums of hermitian matrices (after A. Klyachko), *Séminaire Bourbaki*, exposé 845, juin 1998.

**Hiai (F.), Petz (D.)**, The semicircle law, free random variables and entropy, *Mathematical Surveys and Monographs 77*, American Mathematical Society, Providence, RI, 2000.

**Ledoux (M.)**, The concentration of measure phenomenon, *Mathematical Surveys and Monographs, 89*, American Mathematical Society, Providence, RI, 2001.

**Voiculescu (D.V.)**, Lectures on free probability theory (*Saint-Flour, 1998*), Lecture Notes in Math, 1738, Springer, Berlin, 2000, 279-349.

# Sur le nombre de sommets des polytopes entiers

**Estimer le nombre de points à coordonnées entières dans une région de l'espace est une activité à laquelle se livrent de nombreux mathématiciens et qui possède de multiples applications (géométrie, algèbre, théorie des nombres, optimisation...). On décrit ici ses liens avec la géométrie algébrique moderne... ou comment des problèmes élémentaires d'énoncé éclairent des questions centrales de géométrie algébrique, discipline dont l'accès est (à tort ?) réputé « difficile ».**

Dans tout ce texte, un *polytope entier de dimension  $n$*  est un polytope convexe (encadré 1) de l'espace euclidien  $\mathbf{R}^n$ , non contenu dans un hyperplan et dont les sommets appartiennent au réseau  $\mathbf{Z}^n$  des points dont toutes les coordonnées sont entières. Si  $P$  est un tel polytope, c'est un très vieux problème que d'estimer ou relier le nombre de points entiers  $\text{card}(P \cap \mathbf{Z}^n)$  de  $P$ , le nombre de points entiers  $\text{card}(\overset{\circ}{P} \cap \mathbf{Z}^n)$  dans l'intérieur de  $P$ , le nombre de points entiers  $\text{card}(\partial P \cap \mathbf{Z}^n)$  sur le bord de  $P$  au volume euclidien de  $P$ . Pour le polygone présenté ci-dessous, le lecteur vérifiera que :  $\text{card}(P \cap \mathbf{Z}^2) = 30$ ,  $\text{card}(\overset{\circ}{P} \cap \mathbf{Z}^2) = 20$ ,  $\text{card}(\partial P \cap \mathbf{Z}^2) = 10$  et que l'aire de  $P$  vaut 24 si l'on décide (ce que l'on fera toujours) que l'aire d'une maille élémentaire vaut 1.

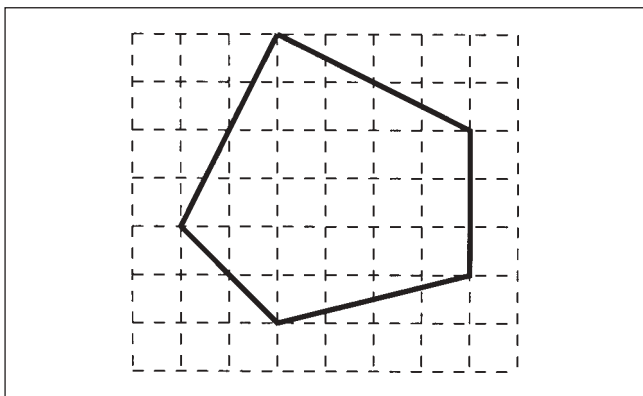


Figure 1 - Un exemple.

Nous énonçons dans la première partie quelques résultats motivés en particulier par la théorie des nombres puis, dans la deuxième partie, quelques résultats très récents, issus de la géométrie algébrique, pour des polytopes entiers particulièrement simples, dits de Fano : ceux possédant 0 comme seul point entier dans l'intérieur, et dont toutes les hyperfaces ont exactement  $n$

sommets formant une base du réseau  $\mathbf{Z}^n$  (encadré 1 pour les notions d'hyperfaces et de base d'un réseau). Modulo les transformations linéaires préservant le réseau  $\mathbf{Z}^n$ , il n'y a qu'un nombre fini de tels polytopes et des bornes précises sur le nombre de leurs sommets sont conjecturées en général et connues en petites dimensions. En associant à tout polytope de Fano une variété algébrique complexe, nous tenterons de faire découvrir au lecteur la *géométrie torique*, permettant d'attaquer les questions précédentes à l'aide de l'attirail moderne de la théorie de Mori.

## QUELQUES RÉSULTATS CLASSIQUES

### Des résultats centenaires

Compter les points entiers d'une partie de l'espace  $\mathbf{R}^n$  est à l'origine une question liée à l'approximation des nombres irrationnels par des nombres rationnels : Gauss obtient 3,14107 comme approximation du nombre  $\pi$  en évaluant à 282 697 le nombre de points entiers dans un disque de rayon 300 centré en 0 ! Cette théorie très ancienne progressa tout particulièrement grâce à Minkowski à la fin du XIX<sup>e</sup> siècle. Pour illustrer un peu mieux les techniques utilisées, nous nous contenterons de démontrer le résultat suivant, élémentaire mais crucial, dû à Blichfeldt (ce dernier fut inspiré par les techniques antérieures de Minkowski mais on lui doit cet énoncé particulièrement frappant).

**Théorème (Blichfeldt, 1914).** Soient  $K$  un compact de l'espace euclidien  $\mathbf{R}^n$  et  $m$  un entier positif. Si  $\text{vol}(K) \geq m$ , il existe au moins  $m + 1$  points distincts  $v_1, \dots, v_{m+1}$  de  $K$  tels que  $v_i - v_j \in \mathbf{Z}^n$  pour tous  $i$  et  $j$ .

La démonstration est très simple : soit  $\mathcal{C}$  le cube élémentaire  $\{x = (x_1, \dots, x_n) \in \mathbf{R}^n \mid 0 \leq x_i \leq 1 \text{ pour tout } i\}$ . Pour  $u \in \mathbf{Z}^n$ , on pose  $K_u = \{x \in \mathcal{C} \mid u + x \in K\}$ . Alors  $\text{vol}(K) = \sum_{u \in \mathbf{Z}^n} \text{vol}(K_u)$ . Supposons pour simplifier que  $\text{vol}(K) > m$ . Comme tous les  $\text{vol}(K_u)$  sont inférieurs ou égaux à 1, on en déduit qu'il y a au moins un point  $x \in \mathcal{C}$  appartenant à  $m + 1$  ensembles  $K_u$ . Autrement dit, il y a  $u_1, \dots, u_{m+1}$  distincts dans  $\mathbf{Z}^n$  tels

– Laurent Bonavero, Institut Fourier – UMR 5582 CNRS – Université Joseph Fourier, BP 74, 38402 Saint Martin d'Hères.  
tél. 04 76 63 58 52, laurent.bonavero@ujf-grenoble.fr

## Encadré 1

# POLYTOPES CONVEXES, SIMPLEXES, BASES D'UN RÉSEAU

Un polytope convexe de l'espace euclidien  $\mathbf{R}^n$  est le plus petit convexe contenant un nombre fini de points donnés. En dimension un, les polytopes convexes sont les segments ; en dimension deux, les polytopes convexes sont appelés polygones convexes, les triangles et les quadrilatères convexes sont des polygones convexes alors qu'un disque n'est pas un polygone convexe ; en dimension trois, les polytopes convexes sont appelés polyèdres convexes. Comme en dimension un, deux ou trois, les polytopes convexes ont des sommets et des faces. Les faces de dimension  $n - 1$  d'un polytope convexe de dimension  $n$  sont appelées hyperfaces (cette notion généralise celle de côté pour les polygones convexes).

Les polygones et polyèdres convexes les plus simples (i.e. avec le moins de sommets et de faces) sont respectivement les triangles et les tétraèdres. Les simplexes généralisent cette notion en dimension  $n$  : ils sont définis comme le plus petit ensemble convexe contenant  $n + 1$  points de  $\mathbf{R}^n$  non contenus dans un hyperplan.

Une famille de  $n$  points du réseau  $\mathbf{Z}^n$  est une base de  $\mathbf{Z}^n$  si tout point de  $\mathbf{Z}^n$  est une combinaison linéaire à coefficients entiers de points de cette famille. Lorsque  $n = 1$ , les deux familles formées du seul élément 1 ou  $-1$  sont les seules

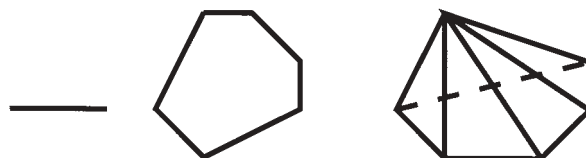


Figure - Un segment, un polygone et un polyèdre.

bases du réseau  $\mathbf{Z}$ . En toute dimension  $n \geq 2$ , il y a une infinité de bases de  $\mathbf{Z}^n$  : si la famille  $\{x_1, x_2\}$  est une base de  $\mathbf{Z}^2$ , la famille  $\{x_1, x_2 + dx_1\}$  est aussi une base de  $\mathbf{Z}^2$  pour tout entier  $d$ .

Les polytopes entiers de  $\mathbf{R}^n$  les plus simples sont les simplexes standard : ce sont les polytopes dont les  $n + 1$  sommets sont 0 et les éléments d'une base du réseau  $\mathbf{Z}^n$ . Ils sont de volume  $1/n!$  et cette propriété les caractérise parmi les simplexes à sommets entiers contenant 0 : en particulier, tout simplexe à sommets entiers est de volume supérieur ou égal à  $1/n!$ .

que  $v_j = x + u_j \in K$ , d'où le résultat. Le cas où  $\text{vol}(K) = m$  se traite en dilatant un peu  $K$  puis en passant à la limite lorsque le coefficient de dilatation décroît vers 1.

**Corollaire (Minkowski).** Soient  $K$  un compact convexe de l'espace euclidien  $\mathbf{R}^n$ , contenant 0 et symétrique par rapport à 0 et  $m$  un entier positif. Si  $\text{vol}(K) \geq m2^n$ , il existe  $m$  paires de points distincts non nuls  $\pm u_j$  appartenant à  $K \cap \mathbf{Z}^n$ .

La démonstration consiste à appliquer le théorème de Blichfeldt à  $\frac{1}{2}K$  et poser  $u_j = v_j - v_{m+1}$  où les  $v_j$  sont donnés par le théorème de Blichfeldt.

L'énoncé précédent assure l'existence de beaucoup de points entiers dans certains compacts convexes si l'on en connaît un et si le volume est suffisamment grand. On attribue généralement à Blichfeldt l'inégalité suivante, qui majore le nombre de points entiers en fonction du volume : si  $K$  est un compact convexe de l'espace euclidien  $\mathbf{R}^n$  contenant 0 et tel que  $K \cap \mathbf{Z}^n$  n'est pas inclus dans un hyperplan,  $\text{card}(K \cap \mathbf{Z}^n) \leq n + n! \text{vol}(K)$ . Donnons-en une preuve (merci à Emmanuel Peyre) : si

$k = \text{card}(K \cap \mathbf{Z}^n) - n$ , considérons un simplexe  $S$  de volume minimal à sommets entiers contenus dans  $K$ . Ce simplexe a un volume au moins égal à  $1/n!$  (encadré 1). Parmi les  $k - 1$  points entiers restant dans  $K$ , choisissons le plus proche de  $S$  et appelons-le  $x_{n+2}$ . Le simplexe  $S'$  engendré par  $x_{n+2}$  et la face de  $S$  la plus proche de  $x_{n+2}$  est de volume au moins égal à  $1/n!$ , d'où  $\text{vol}(K) \geq \text{vol}(S) + \text{vol}(S') \geq 2/n!$ , etc.

### Des estimations plus récentes

Dans ce paragraphe, nous souhaitons estimer le nombre de points entiers sur le bord d'un polytope entier en fonction du nombre de points entiers à l'intérieur. Le premier résultat dans cette direction est le théorème de Pick, en dimension deux, que le lecteur pourra tester sur les polygones de la figure 2.

**Théorème (Pick, 1899).** Si  $P \subset \mathbf{R}^2$  est un polygone convexe entier, alors  $\mathcal{A}(P) = \text{card}(P \cap \mathbf{Z}^2) - \frac{1}{2} \text{card}(\partial P \cap \mathbf{Z}^2) - 1$  où  $\mathcal{A}(P)$  désigne l'aire euclidienne de  $P$ .

La démonstration consiste à traiter d'abord le cas d'un triangle : si  $T$  est un triangle entier dont les seuls points

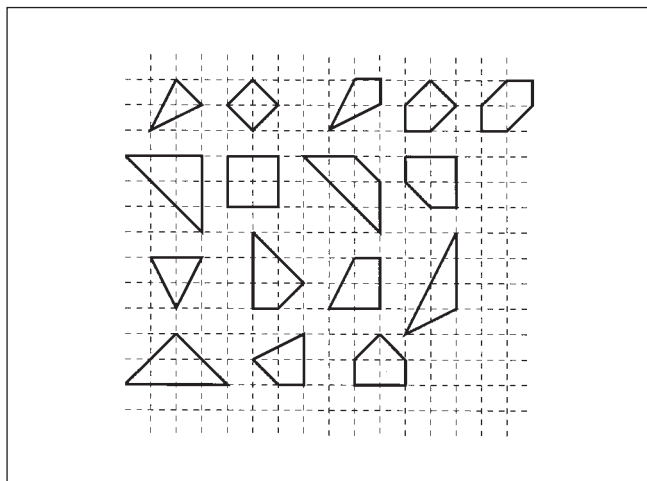


Figure 2 - 16 polygones remarquables.

entiers sont les sommets, alors  $\mathcal{A}(T) = 1/2$ . En effet, si  $A$ ,  $B$  et  $C$  sont les sommets de  $T$ , alors le parallélogramme obtenu par symétrie de  $T$  par rapport au milieu du segment  $BC$  est un parallélogramme dont les seuls points entiers sont les quatre sommets. C'est donc que  $B - A$  et  $C - A$  forment une base du réseau  $\mathbf{Z}^2$ , autrement dit que la matrice  $2 \times 2$  à coefficients entiers dont les colonnes sont les vecteurs  $B - A$  et  $C - A$  est de déterminant  $\pm 1$ , i.e. que le volume du parallélogramme est 1.

Si les seuls points entiers d'un triangle entier sont sur son bord, on déduit de la formule de Pick que  $\text{card}(T \cap \mathbf{Z}^2) = 2\mathcal{A}(T) + 2$  et cette quantité n'est pas bornée comme le montre l'exemple du triangle de sommets  $(0, 0)$ ,  $(0, 1)$  et  $(d, 0)$  ( $d$  entier positif quelconque). Remarquons aussi qu'en dimension trois, il y a des tétraèdres entiers dont les seuls points entiers sont les sommets et de volume arbitrairement grand comme le montre l'exemple du tétraèdre de sommets  $(0, 0, 0)$ ,  $(1, 0, 0)$ ,  $(0, 1, 0)$  et  $(1, 1, d)$  ( $d$  entier positif quelconque).

La situation est complètement différente si l'on impose une valeur non nulle pour le nombre de points entiers à l'intérieur d'un polytope entier comme le montre le résultat suivant.

**Théorème.** Soit  $P$  un polytope entier de dimension  $n$  dont le nombre de points entiers intérieurs  $k := \text{card}(P \cap \mathbf{Z}^n)$  est non nul. Si  $n = 2$ , alors  $\text{card}(P \cap \mathbf{Z}^2) \leq 3k + 7$  (Scott, 1976). Si  $n$  est arbitraire, il existe une constante  $B(k, n)$  ne dépendant que de  $k$  et de  $n$  telle que  $\text{vol}(P) \leq B(k, n)$  (Hensley, 1983 ; Lagarias et Ziegler, 1991).

On en déduit immédiatement le résultat suivant à l'aide de l'inégalité de Blichfeldt.

**Corollaire.** Soit  $P$  un polytope entier de dimension  $n$  tel que  $k = \text{card}(P \cap \mathbf{Z}^n) \geq 1$ . Alors il existe une constante  $B(k, n)$  ne dépendant que de  $k$  et de  $n$  telle que  $\text{card}(P \cap \mathbf{Z}^n) \leq n + n!B(k, n)$ .

Autrement dit, le nombre de points entiers sur le bord d'un polytope entier de dimension  $n$  est contrôlé par le nombre de points entiers à l'intérieur de ce polytope... s'il y en a !

La borne obtenue par Hensley est améliorée par Lagarias et Ziegler qui montrent  $B(k, n) \leq k(7(k + 1))^{n2^{n+1}}$ . Il n'y a à ma connaissance pas de conjecture précise sur ce que pourrait être une borne optimale. Si  $\text{card}(P \cap \mathbf{Z}^n) = 1$ , il y a des exemples, dus à Zaks, Perles et Wilks, de polytopes entiers de dimension  $n$  avec  $\text{vol}(P) \geq 2^{2^{n-1}}/n!$  et  $\text{card}(P \cap \mathbf{Z}^n) \geq 2^{2^{n-2}}$ , l'ordre de grandeur est donc essentiellement optimal. L'idée pour démontrer le résultat de Hensley est la même que pour le résultat de Minkowski : connaissant des points entiers intérieurs, il est possible d'en fabriquer d'autres si le volume est trop grand !

### Un résultat de finitude

Lorsque l'on étudie les polytopes entiers, il faut tenir compte des transformations de l'espace  $\mathbf{R}^n$  préservant le réseau  $\mathbf{Z}^n$  (et donc les notions de points entiers et de polytopes entiers) : ces transformations sont les translations par un vecteur à coordonnées entières et les transformations linéaires  $x \mapsto Ax$  où  $A$  est une matrice de  $\text{GL}_n(\mathbf{Z})$  (i.e. une matrice  $n \times n$  dont les coefficients sont entiers et dont le déterminant est  $\pm 1$  ; une telle matrice préserve donc aussi le volume euclidien). Lagarias et Ziegler déduisent des résultats précédents le théorème de finitude suivant.

**Théorème (Lagarias et Ziegler, 1991).** Pour tout entier  $k \geq 1$ , modulo les translations entières et l'action de  $\text{GL}_n(\mathbf{Z})$ , il n'y a qu'un nombre fini de polytopes entiers de dimension  $n$  dont le nombre de points entiers intérieurs vaut  $k$ .

D'après le théorème de Hensley, le volume d'un polytope entier de dimension  $n$  dont le nombre de points entiers intérieurs vaut  $k$  est majoré par une constante ne dépendant que de  $k$  et  $n$ . Il reste donc à voir qu'il n'y a qu'un nombre fini de tels polytopes, de volume fixé. La démonstration se fait en deux temps. On prouve que si  $K$  est un compact convexe de l'espace euclidien  $\mathbf{R}^n$ , et si  $S$  est un simplexe de volume maximal contenu dans  $K$ , alors  $K \subset (-n)S + (n + 1)s$  où  $s$  est le barycentre de  $S$ . On prouve ensuite que si  $S$  est un simplexe entier de volume  $V$ , alors il y a une matrice  $A \in \text{GL}_n(\mathbf{Z})$  telle que le simplexe  $A(S)$  est inclus dans un cube à sommets



entiers de côté inférieur ou égal à  $n!V$ . On en déduit finalement que pour tout polytope entier  $P$  de volume  $V$ , il y a une matrice  $A \in GL_n(\mathbf{Z})$  telle que le polytope  $A(P)$  est inclus dans un cube à sommets entiers de côté inférieur ou égal à  $nn!V$ . Comme il n'y a qu'un nombre fini de points entiers dans un cube, le résultat s'ensuit.

En dimension deux, il y a, modulo les translations entières et l'action de  $GL_2(\mathbf{Z})$ , 16 polygones entiers possédant exactement un point entier intérieur (figure 2). Il n'y a pas de classification en dimension supérieure ou égale à trois (il faut s'attendre à une liste très longue, rapidement inaccessible !).

### LES POLYTOPES DE FANO

Nous nous intéressons maintenant à une classe de polytopes entiers très simples.

**Définition.** *Un polytope entier de dimension  $n$  est dit de Fano s'il possède 0 comme seul point intérieur et si toutes ses hyperfaces ont exactement  $n$  sommets formant une base du réseau  $\mathbf{Z}^n$ .*

Si  $P$  est un polytope de Fano et si  $f$  est son nombre d'hyperfaces, alors  $P$  est réunion de  $f$  simplexes standard ayant 0 comme sommet commun. De plus, les points entiers du bord de  $P$  sont exactement les sommets. Il découle des résultats précédents de finitude qu'il n'y a, modulo l'action de  $GL_n(\mathbf{Z})$ , qu'un nombre fini de polytopes de Fano de dimension  $n$  et que le nombre de sommets d'un tel polytope est majoré par une constante ne dépendant que de la dimension. Comme souvent en mathématique, la question qui se pose alors est de classer ces objets, au moins en petites dimensions. Le lecteur est encouragé à vérifier que les seuls polygones de Fano sont les cinq premiers de la figure 2.

A chaque polytope de Fano de dimension  $n$ , nous allons associer une variété algébrique complexe de dimension  $n$  après quelques préliminaires de géométrie algébrique.

### Une introduction rapide à la géométrie algébrique (complexe)

#### Variétés algébriques complexes

Dans ce texte, une variété algébrique complexe de dimension  $n$  est un sous-ensemble  $X$  d'un espace projectif complexe  $\mathbf{P}^N(\mathbf{C})$  de dimension  $N$  (pour un entier  $N \geq n$ ) défini par un système d'équations polynomiales homogènes à coefficients complexes, de sorte que tout point  $x$  de  $X$  possède un voisinage dans  $X$  isomorphe à une boule dans  $\mathbf{C}^n$ . Un point d'une variété algébrique complexe de dimension  $n$  est donc repéré localement par des fonctions holomorphes  $x_1, \dots, x_n$  souvent appelées

« coordonnées locales ». En coupant une variété algébrique  $X$  de dimension  $n$  par des hyperplans de l'espace ambiant, on fabrique des sous-variétés de  $X$ , et si l'on coupe  $X$  par  $n - 1$  hyperplans en position générale, on fabrique des sous-variétés de dimension 1 de  $X$ , appelées courbes (pour d'autres précisions, se reporter à l'article de Serge Cantat dans ce numéro).

#### Hypersurfaces canoniques

Il est bien connu que l'étude des formes différentielles sur une variété permet d'en comprendre un peu la géométrie ou la topologie. Dans ce paragraphe (un peu plus technique que le reste de l'article), nous allons associer à toute sous-variété  $Y$  de dimension  $d$  dans une variété complexe  $X$  un nombre noté  $K_X^d \cdot Y$  qui « mesure » l'intersection de l'ensemble des pôles et des zéros d'une forme volume méromorphe sur  $X$  avec la sous-variété  $Y$ .

Si  $X$  est une variété algébrique complexe de dimension  $n$ , considérons une forme différentielle méromorphe  $\omega_X$  de degré maximal (en coordonnées locales,  $\omega_X = f(x)dx_1 \wedge \dots \wedge dx_n$ , où  $f$  est une fonction méromorphe). Cette forme possède des pôles et des zéros localisés le long d'hypersurfaces de  $X$  (i.e des sous-variétés de dimension  $n - 1$  de  $X$ ) : par exemple, la forme  $(x_1^n/x_2^m)dx_1 \wedge dx_2$  a un pôle d'ordre  $m$  le long de l'hyperplan  $\{x_2 = 0\}$  et un zéro d'ordre  $n$  le long de l'hyperplan  $\{x_1 = 0\}$ . A toute forme différentielle méromorphe  $\omega_X$  de degré maximal, on associe une hypersurface canonique de  $X$  de la façon suivante : c'est la somme formelle finie  $K_X := \sum m_i H_i$  où les  $H_i$  sont les hypersurfaces de pôles et de zéros de  $\omega_X$ , et l'entier  $m_i$  est l'ordre du zéro le long de  $H_i$  ou l'opposé de l'ordre du pôle le long de  $H_i$  : dans l'exemple précédent,  $K_X = n\{x_1 = 0\} - m\{x_2 = 0\}$ . Cette hypersurface canonique dépend évidemment du choix de la forme différentielle  $\omega_X$ . En revanche, le théorème des résidus montre que pour toute courbe  $C$  de  $X$ , si l'on note  $H_i \cdot C$  le nombre d'intersection de l'hypersurface  $H_i$  avec la courbe  $C$  (ce nombre est vraiment le nombre de points d'intersection si  $H_i$  et  $C$  se coupent transversalement, sinon il faut tenir compte de l'ordre de contact aux points où  $C$  est tangente à  $H_i$  ; il faut aussi tenir compte des singularités éventuelles de  $C$  et  $H_i$ ), alors l'entier (positif ou négatif)  $K_X \cdot C := \sum m_i H_i \cdot C$  dépend de la courbe  $C$  mais ne dépend pas du choix de la forme différentielle  $\omega_X$ . Plus généralement, si  $Y$  est une sous-variété algébrique de  $X$  de dimension  $d$ , en intersectant  $Y$  avec  $d$  hypersurfaces canoniques, on obtient un entier (positif ou négatif) noté  $K_X^d \cdot Y$ , également indépendant de  $\omega_X$  (voir l'encadré 2 où l'on détaille la situation  $\dim(X) = 1$ ).

#### Variétés de Fano

Parmi les variétés algébriques complexes, une classe se distingue particulièrement : celle des variétés de Fano.

**Encadré 2**

**HYPERSURFACE CANONIQUE DES COURBES ALGÈBRIQUES**

Les courbes algébriques complexes sont topologiquement de trois types (attention, ce sont des objets de dimension 1 complexe, donc de dimension 2 réelle ; on les appelle aussi « surfaces de Riemann ») : la sphère, le tore (ou « bouée à une place ») et le tore à  $g$  trous avec  $g \geq 2$  (ou « bouée multiplaces »). Sur la sphère, il n'y a qu'une structure complexe : celle de la droite projective  $\mathbf{P}^1(\mathbf{C})$ . Sur le tore, les structures complexes sont de la forme  $\mathbf{C}/\Lambda$  où  $\Lambda$  est un réseau de  $\mathbf{C}$  ; en faisant varier  $\Lambda$ , on ne change pas la

structure topologique alors que la structure complexe (ou conforme) varie. On obtient ainsi une famille de dimension complexe 1 de structures complexes sur un même objet topologique. Sur le tore à  $g$  trous, il y a une famille de dimension complexe  $3g - 3$  de structures complexes. Si  $X$  est une courbe algébrique complexe, la formule de Hurwitz permet de calculer la quantité  $K_X \cdot X$  : elle vaut  $-2$  si  $X$  est une sphère,  $0$  si  $X$  est un tore et  $2g - 2$  si  $X$  est un tore à  $g$  trous.

**Définition.** Une variété algébrique complexe  $X$  de dimension  $n$  est de Fano si  $(-1)^d K_X^d \cdot Y > 0$  pour tout entier  $d$  tel que  $1 \leq d \leq n$  et toute sous-variété algébrique  $Y$  de  $X$  de dimension  $d$ .

Si  $X$  est une variété de Fano, on a en particulier  $K_X \cdot C < 0$  pour toute courbe  $C$  de  $X$ . Cela signifie que les formes différentielles méromorphes de degré maximal ont beaucoup plus de pôles que de zéros et, en particulier, qu'il n'y a pas de forme différentielle holomorphe de degré maximal autre que la forme partout nulle. Les exemples les plus simples de variétés de Fano de dimension  $n$  sont  $\mathbf{P}^n(\mathbf{C})$  et les hypersurfaces de degré  $d$  de  $\mathbf{P}^{n+1}(\mathbf{C})$  avec  $1 \leq d \leq n + 1$ .

**Une introduction très rapide à la géométrie torique**

*Variétés toriques*

La géométrie torique, née dans les années 1970, est à l'origine l'étude des variétés algébriques qui sont des compactifications équivariantes du tore complexe  $(\mathbf{C}^*)^n$ . Les plus simples sont  $\mathbf{P}^n(\mathbf{C})$  et  $(\mathbf{P}^1(\mathbf{C}))^n$ , mais il y en a beaucoup d'autres.

**Définition.** Une variété torique est une variété algébrique complexe  $X$  de dimension  $n$  possédant un ouvert dense isomorphe au tore complexe  $T := (\mathbf{C}^*)^n$  de sorte que l'action de  $T$  sur lui-même (par multiplication) se prolonge en une action (algébrique) sur  $X$ .

En particulier, tout  $t \in T$  définit un automorphisme  $\varphi_t$  de la variété algébrique  $X$  et  $\varphi_{t't} = \varphi_t \circ \varphi_{t'}$  pour tous  $t$  et  $t'$  dans  $T$ . Pour alléger les notations, on note généralement  $t \cdot x = \varphi_t(x)$  pour  $t$  dans  $T$  et  $x$  dans  $X$ . Un exemple

important est l'espace projectif de dimension  $n$  : pour  $t = (t_0, \dots, t_{n-1}) \in T$  et  $x = [x_0 : \dots : x_n] \in \mathbf{P}^n(\mathbf{C})$ , on pose  $t \cdot x = [t_0 x_0 : \dots : t_{n-1} x_{n-1} : x_n]$ . Le point essentiel est que les variétés toriques sont codées par des objets combinatoires très simples que nous décrivons maintenant.

*Cônes et éventails*

Un cône rationnel régulier  $\sigma$  de dimension  $r$  de  $\mathbf{R}^n$  est un cône strictement convexe de sommet  $0$  engendré par  $r$  vecteurs  $n_1, \dots, n_r$  de  $\mathbf{Z}^n$  pouvant être complétés en une base du réseau  $\mathbf{Z}^n$ . Le cône  $\sigma$  est donc l'ensemble des combinaisons  $\sum_{i=1}^r \lambda_i n_i$  où les  $\lambda_i$  sont des réels positifs ou nuls. Par exemple, le cône engendré par  $(1, 0)$  et  $(1, 1)$  dans  $\mathbf{R}^2$  est régulier, celui engendré par  $(1, 0)$  et  $(1, 2)$  ne l'est pas puisque la famille  $\{(1, 0), (1, 2)\}$  n'est pas une base de  $\mathbf{Z}^2$ . Un éventail régulier de  $\mathbf{R}^n$  est une collection finie  $\Delta$  de cônes rationnels réguliers recouvrant  $\mathbf{R}^n$  et vérifiant les deux conditions suivantes : si  $\sigma$  appartient à  $\Delta$ , alors toutes ses faces sont dans  $\Delta$  (remarquer que  $0$  est face de tout cône), et si  $\sigma$  et  $\sigma'$  appartiennent à  $\Delta$ , alors  $\sigma \cap \sigma'$  est une face commune de  $\sigma$  et  $\sigma'$ . Voici deux éventails de  $\mathbf{R}^2$ , le premier est constitué de 7 cônes (3 de dimension deux, 3 de dimension un et 1 de dimension zéro), le second de 9 cônes.

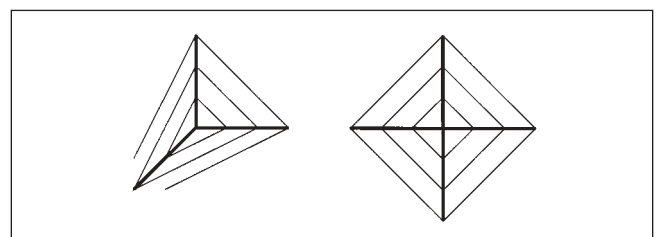


Figure 3 - Deux éventails de  $\mathbf{R}^2$ .

Soit  $X$  une variété torique de dimension  $n$ . Comme  $T \subset X$ , il y a dans  $X$  un point particulier :  $x_e = (1, \dots, 1) \in T \subset X$ . Pour chaque  $v \in \mathbf{Z}^n$ , il y a une action du tore  $\mathbf{C}^*$  de dimension 1 sur  $X$  définie par  $z \cdot_v x = (z^{v_1}, \dots, z^{v_n}) \cdot x$  où  $z \in \mathbf{C}^*$ ,  $x \in X$  et  $v_1, \dots, v_n$  sont les coordonnées (entières) de  $v$ . Nous construisons un éventail en regardant les limites possibles (lorsque  $z$  tend vers 0) lorsque  $v$  décrit  $\mathbf{Z}^n$  des orbites du point  $x_e$ . Comme  $X$  est compacte et l'action algébrique,  $\lim_{z \rightarrow 0} (z \cdot_v x_e)$  existe dans  $X$  et l'observation clé est la suivante :

**Proposition.** *Il y a un éventail  $\Delta_X$  tel que l'ensemble des  $C_x := \{v \in \mathbf{Z}^n \mid \lim_{z \rightarrow 0} (z \cdot_v x_e) = x\}$  lorsque  $x$  décrit  $X$  est exactement l'ensemble (fini) des  $\overset{\circ}{\sigma} \cap \mathbf{Z}^n$  lorsque  $\sigma$  décrit  $\Delta_X$  (où  $\overset{\circ}{\sigma}$  est l'intérieur de  $\sigma$  dans l'espace vectoriel engendré par  $\sigma$ ).*

Nous ne démontrons pas cette proposition ici mais nous encourageons vivement le lecteur à vérifier que le premier éventail de la figure 3 est celui du plan projectif  $\mathbf{P}^2(\mathbf{C})$  et le deuxième celui de  $\mathbf{P}^1(\mathbf{C}) \times \mathbf{P}^1(\mathbf{C})$ .

Cette construction admet une réciproque : tout éventail régulier détermine une variété torique.

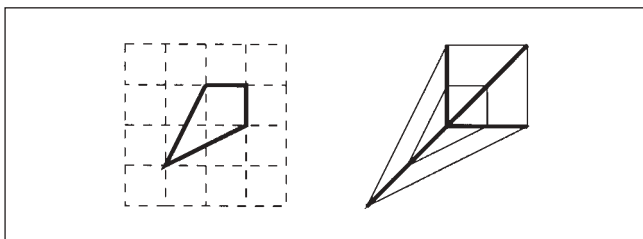


Figure 4 - Un polygone de Fano et l'éventail associé.

Il est maintenant grand temps de revenir aux polytopes...

### Variétés de Fano toriques

A tout polytope de Fano  $P$  est naturellement associé un éventail régulier de la façon suivante : pour chaque hyperface  $F$  de  $P$ , le cône de sommet 0 et s'appuyant sur  $F$  est un cône régulier. La collection de tous ces cônes et de leurs faces est clairement un éventail régulier (figure 4).

D'après ce qui précède,  $P$  détermine donc une variété torique  $X_P$  et il n'est pas très difficile de démontrer la proposition suivante, que le lecteur a sans doute déjà devinée.

**Proposition.** *Il y a une correspondance bijective entre les polytopes de Fano de dimension  $n$  et les variétés de Fano toriques de dimension  $n$ .*

En utilisant à la fois des méthodes combinatoires et des méthodes venant de la théorie de Mori (encadré 4), il est possible de donner une liste de toutes les variétés de Fano toriques de dimension inférieure ou égale à 4 : il n'y a que  $\mathbf{P}^1$  en dimension 1 et respectivement 5, 18 et 124 variétés de Fano toriques de dimension respectivement 2, 3 et 4. Ces classifications sont dues à Watanabe, Watanabe et Batyrev en dimension 3 et à Batyrev et Sato en dimension 4. Dans le cas des surfaces de Fano toriques, nous avons déjà mentionné que les polygones de Fano associés sont les 5 premiers de la figure 2 (encadré 3).

En utilisant ces résultats de classification, on remarque qu'un polytope de Fano de dimension respectivement 1, 2, 3 ou 4 possède au plus 2, 6, 8 ou 12 sommets respectivement. Ces résultats vont dans le sens d'une conjecture de Batyrev que nous énonçons maintenant.

### Encadré 3

## ÉCLATEMENTS ET SURFACES DE FANO TORIQUES

Si  $S$  est une surface complexe et  $x$  un point de  $S$ , il y a un procédé essentiel en géométrie algébrique permettant de construire une nouvelle surface  $S_x$  en remplaçant le point  $x$  par la droite projective des directions tangentes à  $S$  en  $x$  : ce procédé est local car il ne modifie  $S$  qu'au voisinage de  $x$  et on dit qu'on éclate le point  $x$  dans  $S$ . Le modèle local est le suivant : souvenons nous que  $\mathbf{P}^1$  est naturellement l'ensemble des droites vectorielles de  $\mathbf{C}^2$ , l'éclatement de 0 dans  $\mathbf{C}^2$  est la

surface  $(\mathbf{C}^2)_0$  définie par :  $(\mathbf{C}^2)_0 = \{(v, d) \in \mathbf{C}^2 \times \mathbf{P}^1 \mid v \in d\}$ . La structure complexe de la variété  $S_x$  dépend du choix de  $x$  mais sa topologie n'en dépend pas : en faisant varier  $x$  dans  $S$ , on obtient un exemple de famille de structures complexes. Les 5 surfaces de Fano toriques sont  $\mathbf{P}^2$ ,  $\mathbf{P}^1 \times \mathbf{P}^1$  et les surfaces obtenues en éclatant respectivement un, deux ou trois points fixes du tore dans  $\mathbf{P}^2$ .

**Conjecture (Batyrev, 1988).** *Tout polytope de Fano de dimension  $n$  possède au plus  $3n$  sommets si  $n$  est pair et  $3n - 1$  sommets si  $n$  est impair.*

On peut remarquer que ces bornes sont beaucoup plus petites que celles données par le résultat de Hensley. Debarre a montré très récemment que *le nombre de sommets d'un polytope de Fano de dimension  $n$  est inférieur ou égal à  $n + 2 + 2\sqrt{(n^2 - 1)(2n - 1)}$*  et Casagrande a démontré la conjecture de Batyrev en dimension 5 (où il n'y a pas de classification). A nouveau, les techniques de Casagrande viennent de la géométrie torique. Nous avons besoin pour cela d'une notion supplémentaire de la géométrie algébrique.

Si  $X$  est une sous-variété algébrique d'un espace projectif complexe, considérons l'espace vectoriel des combinaisons finies  $\sum a_i C_i$  où les  $a_i$  sont des nombres réels et les  $C_i$  des courbes de  $X$ . Cet espace est de dimension infinie mais devient de dimension finie si l'on identifie deux combinaisons  $\sum a_i C_i$  et  $\sum b_i C_i$  si et seulement si pour toute hypersurface  $H$  de  $X$ , on a  $\sum a_i C_i \cdot H = \sum b_i C_i \cdot H$  (par exemple, dans  $\mathbf{P}^2(\mathbf{C})$ , deux courbes sont identifiées si leurs nombre d'intersection avec toute droite sont égaux, autrement dit si elles ont le même degré). La dimension de l'espace ainsi obtenu est appelée *nombre de Picard* de la variété  $X$  et est notée généralement  $\rho_X$ .

Pour une variété de Fano torique  $X_P$  de dimension  $n$  dont le polytope de Fano associé est  $P$ , le nombre de sommets de  $P$  est égal à  $n + \rho_{X_P}$ , si bien que la con-

jecture de Batyrev se reformule ainsi : *le nombre de Picard d'une variété de Fano torique de dimension  $n$  est inférieur ou égal à  $2n$  si  $n$  est pair et à  $2n - 1$  si  $n$  est impair.*

Il n'y a à ma connaissance pas de conjecture précise sur le nombre de Picard d'une variété de Fano arbitraire (i.e. non torique) mais on s'attend à une borne linéaire vis-à-vis de la dimension.

#### CONCLUSION

Ces dernières années, de nombreuses conjectures de la géométrie algébrique ont été testées sur les variétés toriques et, pour certaines, démontrées à l'aide de la géométrie torique. Cependant, de nombreuses questions restent encore ouvertes. Donnons-en une parmi tant d'autres pour conclure ce texte.

Soit  $X$  une variété algébrique complexe telle que  $K_X \cdot C \leq 0$  pour toute courbe  $C$  de  $X$ . Le théorème de Hensley montre qu'il n'y a qu'un nombre fini de telles variétés *toriques* de dimension donnée. La question analogue dans le monde non torique serait la suivante : *y a-t-il un nombre fini de types de déformation de telles variétés de dimension donnée ?* Cette question est redoutablement difficile et complètement ouverte dès la dimension trois, y compris pour les variétés de Calabi-Yau, chères à certains physiciens (ce sont des variétés de dimension trois telles que  $K_X \cdot C = 0$  pour toute courbe  $C$ ) et ce, malgré des dizaines de travaux sur le sujet ces dix dernières années !

#### Encadré 4

### VARIÉTÉS DE FANO ET THÉORIE DE MORI

*Les variétés de Fano occupent une place essentielle dans la théorie communément appelée « géométrie algébrique de dimension supérieure » (sous-entendu : supérieure ou égale à trois) depuis une vingtaine d'années et les travaux pionniers de Mori. L'idée de Mori est d'étudier une variété algébrique  $X$  à l'aide des courbes  $C$  de  $X$  telles que  $K_X \cdot C < 0$  et de montrer qu'après un nombre fini de « chirurgies biméromorphes », il y a une application  $f : X \rightarrow Z$  où  $Z$  est une variété algébrique de dimension plus petite telle que  $K_Z \cdot C \geq 0$  pour toute courbe de  $Z$  et telle que les fibres de  $f$  sont des variétés de Fano (en un sens un peu plus général que celui de la définition ci-dessus), les variétés de Fano sont donc des « briques élémentaires » dans la classification des variétés algébriques. Ce programme dit « programme du modèle minimal » ou encore « programme de Mori » est achevé jusqu'en dimension trois et a valu la médaille Fields à Mori. En toute dimension, les travaux de Nadel, Campana et*

*de Kollár, Miyaoka et Mori montrent au début des années 1990 le résultat fondamental suivant : il n'y a qu'un nombre fini de types de déformation de variétés (complexes) de Fano de dimension fixée. En dimension inférieure ou égale à trois, des classifications complètes existent : il n'y a qu'une courbe de Fano (la droite projective  $\mathbf{P}^1(\mathbf{C})$ ), 10 familles de surfaces de Fano (il s'agit de  $\mathbf{P}^1 \times \mathbf{P}^1$  et de  $\mathbf{P}^2$  éclaté en au plus 8 points en position générale, voir l'encadré 3 pour cette notion), 105 familles de variétés de Fano de dimension trois, ces dernières ont été classifiées par Iskovskih, Mori et Mukai (mentionnons au lecteur que Mori a annoncé en septembre 2002 l'existence de la 105<sup>e</sup> famille de variétés de Fano de dimension trois, la classification publiée il y a une vingtaine d'années n'en comportait que 104 !). La démonstration de ces résultats utilise tout l'attirail de la géométrie algébrique moderne.*

## POUR EN SAVOIR PLUS

**Bonavero (L.)**, Factorisation faible des applications birationnelles, d'après Abramovich *et al.*, *Séminaire Bourbaki*, Volume 2000/2001, Paris, Société mathématique de France, Astérisque No. 282, Exp. N° 880, 2002, 1-37.

**Brion (M.)**, Points entiers dans les polytopes convexes, *Séminaire Bourbaki*, Volume 1993/94, Paris, Société mathématique de France, Astérisque N° 227, Exp. N° 780, 1995, 145-169.

**Cassels (J.W.S.)**, An Introduction to the Geometry of Numbers, *Die Grundlehren der mathematischen Wissenschaften*, Bd. 99 Springer-Verlag, Berlin-Göttingen-Heidelberg, 1959.

**Debarre (O.)**, Higher-dimensional algebraic geometry, *Universitext*, Springer-Verlag, New York, 2001.

**Ewald (G.)**, Combinatorial Convexity and Algebraic Geometry, *Graduate Texts in Mathematics*, N° 168, Springer-Verlag, New York, 1996.

**Lagarias (J.-C.), Ziegler (G.)**, Bounds for lattice polytopes containing a fixed number of interior points in a sublattice, *Canad. J. Math.* 43, n° 5, 1991, 1022-1035.

**Oda (T.)**, Convex Bodies and Algebraic Geometry: an Introduction to the Theory of Toric Varieties, *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.*, 015. Springer, 1988.

**Wiśniewski (J.-A.)**, Toric Mori Theory and Fano Manifolds, dans *Geometry of Toric Varieties*, Laurent Bonavero – Michel Brion (Ed.) *Séminaires et Congrès* 6, 2002, 249-272.

---

### Note de l'auteur

Je remercie tous ceux qui ont critiqué les premières versions de ce texte.

# Dynamique diophantienne

**Comme souvent, un problème de nature arithmétique mène à des questions qui relèvent des systèmes dynamiques. Il s'agit de décrire les trajectoires de transformations polynomiales sur l'espace des solutions de certaines équations algébriques.**

## GÉOMÉTRIE DIOPHANTINNE ET DYNAMIQUE

La géométrie diophantienne s'attache à décrire les solutions en nombres entiers d'équations polynomiales. L'exemple le plus connu est l'équation de Fermat

$$x^n + y^n = z^n,$$

$n$  étant un entier positif fixé,  $x$ ,  $y$  et  $z$  étant les inconnues. Lorsque  $n$  vaut 2, l'équation correspond à la relation de Pythagore pour les côtés d'un triangle rectangle ; il existe alors une infinité de solutions, notamment

$$x = p^2 - q^2, \quad y = 2pq, \quad z = p^2 + q^2,$$

où  $p$  et  $q$  parcourent l'ensemble des nombres entiers. En revanche, lorsque  $n$  est supérieur ou égal à 3, Wiles a récemment démontré qu'il n'existe aucune solution en nombres entiers strictement positifs. Un deuxième exemple, moins médiatique mais tout aussi important, est fourni par l'équation de Markov

$$x^2 + y^2 + z^2 = 3xyz.$$

Là encore, il existe une infinité de solutions en nombres entiers. Le triplet  $(1, 1, 1)$  est une solution évidente et Markov a montré que toutes les autres s'obtiennent à partir de cette solution particulière en appliquant les trois transformations

$$\begin{cases} \alpha(x, y, z) = (3yz - x, y, z) \\ \beta(x, y, z) = (x, 3zx - y, z) \\ \gamma(x, y, z) = (x, y, 3xy - z) \end{cases}.$$

En guise d'illustration, appliquons successivement les transformations  $\alpha$ ,  $\beta$  et  $\gamma$  et itérons ce procédé deux fois. La solution obtenue est

$$(433, 37\,666, 48\,928\,105).$$

---

– Serge Cantat, Institut de recherche mathématique de Rennes – UMR 6625 CNRS – Université Rennes 1, campus de Beaulieu, bât. 22, avenue du général Leclerc, 35042 Rennes cedex  
serge.cantat@univ-rennes1.fr

Une partie importante des équations polynomiales qui possèdent une infinité de solutions entières relèvent de la même philosophie que l'équation de Markov : des transformations polynomiales (analogues à  $\alpha$ ,  $\beta$  et  $\gamma$ ) produisent une infinité de solutions à partir d'une seule. Le lecteur curieux (ou savant) pourra d'ailleurs s'assurer que les triplets pythagoriciens entrent dans ce cadre. Pour ce type d'équations, l'arithmétique rejoint la dynamique : comprendre la structure des solutions entières de l'équation revient, en partie, à décrire l'action des transformations polynomiales. C'est cette relation entre dynamique et arithmétique que nous voulons illustrer ici. Des constructions de nature arithmétique permettent en effet d'obtenir des résultats sur la dynamique.

Dans la suite, nous emploierons le vocabulaire géométrique présenté dans l'encart ci-dessous. La variété étudiée sera projective et l'étude de ses points entiers sera donc équivalente à celle de ses points rationnels. La surface définie par l'équation de Markov n'entre pas dans ce cadre et nous donnerons des énoncés spécifiques à son cas.

---

## VARIÉTÉS PROJECTIVES

Par définition, l'ensemble des solutions  $(x_0, \dots, x_k)$  d'un système d'équations polynomiales est une variété algébrique (affine) et chaque solution est un point de la variété. En fait, une équation donne simultanément naissance à plusieurs variétés suivant que l'on considère les solutions en nombres entiers, rationnels, réels, complexes... Nous précisons en indice l'espace dans lequel varient les solutions qui nous intéressent, par exemple  $V_{\mathbb{C}}$  pour les points complexes de la variété  $V$ . Lorsque les équations qui déterminent la variété  $V$  sont homogènes, tout point  $(x, y, \dots)$  de  $V$  est associé à une infinité de solutions  $(ax, ay, \dots)$  où  $a$  varie dans  $\mathbf{Z}$  (ou dans  $\mathbf{Q}$ ,  $\mathbf{R}$ , ...). Autrement dit, si  $m$  est un point de  $V$ , la droite joignant l'origine à  $m$  est contenue dans  $V$ . L'objet naturel est donc l'ensemble des droites passant par l'origine et contenues dans  $V$ . Il s'agit d'une partie de l'espace projectif (l'espace de toutes les droites vectorielles) ; on parle donc de variété projective. Les coordonnées  $[x : y : \dots]$  d'un point de l'espace projectif  $\mathbf{P}^k$  sont déterminées à un facteur multiplicatif «  $a$  » près. Un point à coordonnées rationnelles est donc équivalent à un point à coordonnées entières : il suffit de multiplier chaque coordonnée par le produit de leurs dénominateurs.

---

## COMPTER LES POINTS ET LES ITÉRER

Les variétés projectives qui possèdent une infinité de points rationnels en possèdent une quantité dénombrable. En ce sens, elles ont toutes exactement le même nombre de points. Certaines en ont cependant plus que d'autres et, pour s'en convaincre, nous allons les compter.

Chaque point rationnel  $m$  de l'espace projectif peut être représenté par des coordonnées entières sans facteur premier commun. Il y a exactement deux écritures de ce type,  $[x : y : \dots]$  et  $[-x : -y : \dots]$ , ce qui permet de définir la *hauteur (multiplicative)* de  $m$  par la formule

$$H(m) = \max(|x|, |y|, \dots)$$

et sa *hauteur logarithmique* (ou *additive*)  $h(m) = \log(H(m))$ . Si  $V$  est une variété projective, le nombre de points de  $V_{\mathbf{Z}}$  dont la hauteur multiplicative est plus petite que  $B$  est noté  $N_V(B)$ . Cela définit la *fonction de comptage* de  $V_{\mathbf{Z}}$ . Lorsque  $V_{\mathbf{Z}}$  possède une infinité de points, cette fonction croît avec  $B$  jusqu'à l'infini. Plus cette croissance est rapide, plus il y a de points rationnels.

L'exemple le plus simple est celui de l'espace projectif  $V = \mathbf{P}^k$ . En notant  $\zeta(q)$  la somme des inverses des puissances  $q^{\text{èmes}}$  des nombres entiers positifs, Schanuel a montré que

$$N_{\mathbf{P}^k}(B) \simeq \frac{2^k}{\zeta(k+1)} B^{k+1}$$

avec une erreur majorée par  $B^k$  (ou  $B \log(B)$  si  $k = 1$ ). Pour la surface de Markov  $M$ , le dénombrement des points entiers de hauteur plus petite que  $B$  a été effectué par Zagier,

$$N_M(B) \simeq \gamma \log^2(3B), \text{ où } \gamma \simeq 0,18$$

avec une erreur majorée par  $\log(B) \log(\log(B))$ . Des conjectures précises relatives au comportement asymptotique de la fonction de comptage  $N_V(B)$  ont été formulées par Batyrev, Manin et Peyre lorsque la géométrie de  $V$  ressemble à celle de l'espace projectif, c'est-à-dire, en termes techniques, lorsque le fibré canonique de  $V$  est suffisamment négatif.

Revenons maintenant aux variétés projectives dont les points rationnels sont permutés par une transformation  $f : V \rightarrow V$  qui est polynomiale. Le décompte des points rationnels de  $V$  peut alors être scindé en deux calculs distincts : compter le nombre de trajectoires de  $f$  et évaluer la hauteur des points le long de chaque trajectoire  $m, f(m), f(f(m)) \dots$ . Concentrons-nous sur cette deuxième étape, car c'est elle qui nous conduira à des questions intéressantes de systèmes dynamiques. Nous avons déjà vu un exemple au premier paragraphe avec la transfor-

mation  $f = \alpha \circ \beta \circ \gamma$  sur la surface de Markov : le point  $(1, 1, 1)$ , de hauteur égale à 1, s'élève à la hauteur

$$H(f^2(1, 1, 1)) = 48\,928\,105$$

après deux itérations et à la hauteur approximative  $35 \cdot 10^{47200}$  après seulement huit itérations.

Afin d'énoncer des résultats précis, nous allons maintenant décrire ce qui se produit pour les exemples des encadrés 1 et 2. Il y a une différence essentielle entre ces deux exemples : la transformation  $f$  de l'encadré 1 est inversible, c'est-à-dire que tout point  $m$  est l'image par  $f$  d'un unique point  $f^{-1}(m)$ , la transformation  $g$  ne l'est pas. Les constructions valables pour  $f$  et  $g$  le seront donc pour  $f^{-1}$ . La dynamique de ces transformations est très riche. La première façon de mesurer cette complexité est de regarder la suite des degrés des polynômes obtenus en itérant ces transformations. Pour cela, nous noterons  $\lambda_F$  le nombre positif réel

$$\lambda_F = \limsup_{n \rightarrow \infty} \{\deg(F^n)^{1/n}\},$$

$F$  étant  $f, f^{-1}$  ou  $g$  et  $\deg(F^n)$  désignant le degré des polynômes qui définissent la transformation  $F^n$ . Il se trouve que, sur ces exemples,  $\lambda_F$  est strictement plus grand que 1 (encadrés 1 et 2).

Une astuce classique introduite par Néron et Tate dans ce cadre permet d'évaluer la hauteur le long des trajectoires : on change la fonction de hauteur pour l'adapter à la dynamique. En pratique, il s'agit de poser

$$h^+(m) = \lim_{n \rightarrow \infty} \left( \frac{1}{(\lambda_F)^n} h(F^n(m)) \right)$$

où  $F$  doit être remplacée par  $f$  ou  $g$ . Puisque  $f$  est inversible,  $F$  peut également être remplacée par  $f^{-1}$  ce qui définit une seconde hauteur  $h^-$ . Ces nouvelles fonctions de hauteur vérifient l'équation fonctionnelle  $h^+ \circ F = \lambda_F h^+$  ; en particulier, le long d'une trajectoire on obtient

$$h^+(F^n(m)) = (\lambda_F)^n h^+(m).$$

Call et Silverman ont montré que ces hauteurs adaptées à la dynamique sont bien définies et permettent de retrouver l'essentiel de la hauteur usuelle  $h$ . Ainsi, dans le cas de  $f$ , la différence entre  $h$  et la somme  $h^+ + h^-$  est bornée. Le long des trajectoires infinies de  $f$ ,  $h(f^n(m))$  croît donc comme  $(\lambda_f)^n$ .

Le second point important est que  $h^+$  est nulle précisément sur les points rationnels qui ont une orbite finie. Une relation intéressante apparaît donc entre arithmétique et dynamique. Nous allons maintenant décrire une application bien plus délicate de ces hauteurs mais, auparavant, expliquons la signification dynamique du nombre  $\lambda_F$ .

Encadré 1

## SURFACES TRIPLEMENT DE DEGRÉ 2

Reprenons les notations de l'introduction concernant la surface de Markov, munie des trois involutions  $\alpha$ ,  $\beta$  et  $\gamma$ . L'équation de cette surface est

$$x^2 + y^2 + z^2 = 3xyz.$$

Nous noterons  $M$  la partie de cette surface constituée des points dont toutes les coordonnées sont positives. On peut paramétrer  $M$  par l'intérieur d'un triangle : si  $(u, v, w)$  sont les coordonnées barycentriques d'un point du triangle, l'élément de la surface de Markov est  $(\Delta u, \Delta v, \Delta w)$  où  $\Delta = (u^2 + v^2 + w^2)/(3uvw)$ . Ce changement de variables permet donc de visualiser la dynamique des transformations  $\alpha$ ,  $\beta$  et  $\gamma$  en faisant des dessins dans un triangle.

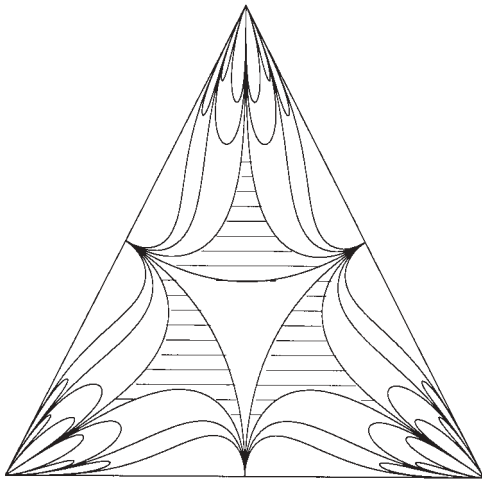


Figure 1 - Les trois involutions envoient le « pavé » central délimité par trois arcs de cercles sur les trois zones hachurées adjacentes ; en composant successivement ces involutions entre elles, ce « pavé » engendre ainsi un pavage biscornu du triangle (figure réalisée par Benoît Kloeckner).

Voici maintenant une façon de déformer l'exemple de Markov pour obtenir une dynamique compliquée sur des surfaces algébriques réelles. Soit  $P(x, y, z)$  un polynôme en trois variables dont le degré par rapport à chacune des variables est égal à 2. Autrement dit, lorsque l'on fixe deux des variables, on obtient un polynôme de degré 2 par rapport à la variable restante.

Notons  $S_0(P)$  la variété associée à l'équation  $P$ , et considérons son adhérence (compacte)  $S(P)$  dans  $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$ . Cela détermine une surface projective, car  $\mathbf{P}^1 \times \mathbf{P}^1 \times \mathbf{P}^1$  est une variété projective. Nous supposons que cette surface est lisse. Ce n'est pas une hypothèse anodine ; elle est vérifiée pour la plupart des polynômes  $P$  mais elle ne l'est pas pour la surface de Markov.

Puisque le degré de  $P$  par rapport à  $x$  est égal à 2, chaque point  $(x, y, z)$  est associé à un second,  $\alpha(x, y, z) = (x', y, z)$ , où  $x'$  est la seconde solution de  $P$  lorsque  $y$  et  $z$  sont fixés. Cela détermine une transformation polynomiale de  $S$  qui est involutive :  $\alpha \circ \alpha = \text{id}_S$ . De même, en privilégiant respectivement  $y$  et  $z$ , on définit deux autres involutions  $\beta$  et  $\gamma$ . Par composition,  $\alpha$ ,  $\beta$  et  $\gamma$  engendrent un groupe de transformations polynomiales de  $S$ . Lorsque les coefficients de  $P$  sont rationnels, ces transformations polynomiales sont définies par des polynômes à coefficients rationnels : elles permutent donc les points de  $S(P)_{\mathbf{Q}}$ . Nous noterons  $f$  la transformation obtenue en composant successivement les trois involutions :

$$f = \alpha \circ \beta \circ \gamma.$$

La dynamique de cette transformation est extrêmement complexe, comme on peut le voir sur la figure suivante :

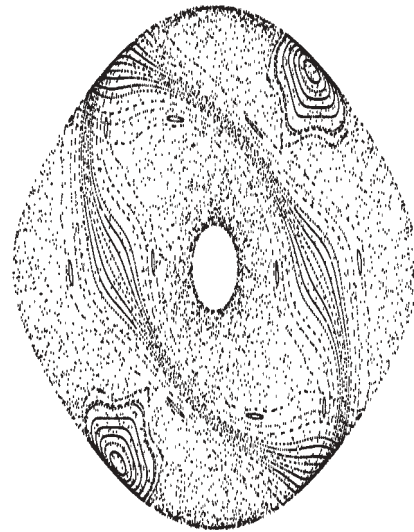


Figure 2 - Plusieurs orbites (réelles) pour la transformation  $f$ . Sur cet exemple, le polynôme  $P$  est à coefficients rationnels et nous avons tracé des orbites de points réels. La surface  $S_{\mathbf{R}}$  est homéomorphe à un tore. Les orbites ont été tracées en entier (certaines passent donc du côté « caché » de la surface).

Une façon de mettre en évidence la complexité de cette dynamique est de regarder les polynômes qui définissent les transformations  $f^n$ ,  $n = 1, 2, \dots$ . Il se trouve que leur degré croît comme  $(9 + 4\sqrt{5})^n$ . Ce nombre  $\lambda_f = 9 + 4\sqrt{5}$  joue un rôle crucial dans l'étude des propriétés dynamiques de  $f$  (voir le corps du texte).



## LE FACTEUR $\lambda_F$ DONNE L'ENTROPIE

Lorsque l'on dispose d'un système dynamique un tant soit peu compliqué, il est illusoire de vouloir décrire l'évolution de toutes les trajectoires. La première stratégie est alors de décrire les orbites les plus simples, à savoir les orbites périodiques. La seconde consiste à adopter un point de vue probabiliste ; il s'agit de décrire le comportement asymptotique de presque toute trajectoire. En ce qui nous concerne, les deux points de vue vont se rejoindre.

Avant toute chose, il convient d'interpréter en termes dynamiques le coefficient  $\lambda_F$  qui décrivait l'évolution de la hauteur le long d'une trajectoire. Définissons pour cela l'entropie topologique de la transformation  $F$ . Soit  $\varepsilon$  un nombre réel, strictement positif mais très petit ; ce nombre représente la précision à laquelle nous observons le système : plus  $\varepsilon$  est petit plus la précision est grande. Pour tout entier positif  $n$ , notons  $T(n, \varepsilon)$  le nombre maximum de trajectoires de longueur  $n$  qui peuvent être distinguées à la précision  $\varepsilon$  : les trajectoires des points  $m_1$  et  $m_2$  sont discernables s'il existe un instant  $k$  compris entre 0 et  $n$  pour lequel  $F^k(m_1)$  et  $F^k(m_2)$  sont à une distance supérieure à  $\varepsilon$ . En général, la suite  $T(n, \varepsilon)$  croît exponentiellement vite avec  $n$ . On pose donc

$$h_\varepsilon(F) = \limsup_{n \rightarrow \infty} \left( \frac{1}{n} \log(T(n, \varepsilon)) \right)$$

et l'on définit l'entropie topologique  $h_{top}(F)$  en prenant la limite de  $h_\varepsilon(F)$  lorsque la précision devient infiniment grande (i.e.  $\varepsilon$  tend vers 0). L'entropie topologique mesure donc le « nombre asymptotique de trajectoires distinctes ».

Lorsque  $F$  coïncide avec l'une des transformations  $f$  ou  $g$  des encadrés 1 et 2, les travaux de Yomdin et Gromov montrent que l'entropie est égale au logarithme du nombre  $\lambda_F$  :

$$h_{top}(F) = \log(\lambda_F)$$

( $F$  étant une transformation de  $V_C$ ). En d'autres termes, prenez un point entier, itérez-le et regardez à quelle vitesse ses coordonnées tendent vers l'infini – vous obtenez alors le « nombre asymptotique de trajectoires » de  $F$ .

Dans les cas qui nous préoccupent, l'entropie topologique est strictement positive, car  $\lambda_F$  est strictement supérieur à 1. La dynamique est donc très riche, en particulier  $F$  possède une infinité de points périodiques hyperboliques (si  $F = f$ ) ou répulsifs (si  $F = g$ ). C'est pour comprendre la répartition de ces points périodiques que les hauteurs adaptées vont être utiles. Pour cela, il est nécessaire de séparer la hauteur  $h^+$  construite au deuxième paragraphe en une somme de hauteurs locales  $h_p^+$  ...

## POINTS PÉRIODIQUES

Un point  $m$  est dit périodique s'il existe un entier  $k$  strictement positif tel que  $F^k(m) = m$ . Le plus petit entier  $k$  qui convient s'appelle la période de  $m$ .

Le point est de type hyperbolique si les modules des valeurs propres de la différentielle de  $F^k$  au point  $m$  sont, pour une part, strictement plus grands que 1 et, pour une autre part, strictement plus petits que 1. Le point est répulsif si tous les modules des valeurs propres sont plus grands que 1.

## LA FORMULE DU PRODUIT

Soit  $\mathcal{P}$  l'ensemble des nombres premiers et  $p$  un élément de  $\mathcal{P}$ . Si  $q$  est un nombre entier, sa valuation  $p$ -adique  $v_p(q)$  est définie comme le plus grand nombre entier positif  $k$  tel que  $p^k$  divise  $q$ . Ainsi,

$$q = \prod_{p \in \mathcal{P}} p^{v_p(q)}. \quad (1)$$

Nous utiliserons également la norme  $p$ -adique  $\|q\|_p = (1/p)^{v_p(q)}$ . Cette norme est égale à 1 si  $p$  ne divise pas  $q$  et est d'autant plus petite que  $p$  divise  $q$ . Les entiers  $p$ -adiques sont définis en complétant  $\mathbf{Z}$  relativement à cette norme. Autrement dit, on adjoint aux entiers les limites de suites qui convergent dans la norme  $p$ -adique, par exemple le nombre 3-adique

$$\lim_{n \rightarrow \infty} (1 + 3^2 + 3^4 + \dots + 3^{2^n}).$$

Les nombres réels peuvent être introduits de manière analogue en complétant les nombres rationnels pour la valeur absolue usuelle, à savoir  $\|q\|_\infty = |q|$ . Lorsqu'une variété  $V$  est définie par des équations à coefficients entiers, on peut donc la considérer alternativement comme une variété sur les réels  $V_{\mathbf{R}}$  ou sur les  $p$ -adiques  $V_{\mathbf{Q}_p}$ .

Dans le contexte simple où nous nous plaçons, la formule du produit consiste à évaluer la valeur absolue d'un entier  $q$  à l'aide de la formule de décomposition en facteurs premiers (1) :

$$\|q\|_\infty = \prod_{p \in \mathcal{P}} (\|q\|_p)^{-1}.$$

On en déduit sans peine que la hauteur  $h(m)$  d'un point  $m = [x : y : \dots]$  de l'espace projectif est une somme  $h(m) = \sum_{p \in \mathcal{P} \cup \infty} h_p(m)$  de hauteurs locales  $h_p(m)$  valant chacune

$$\max(\log(\|x\|_p), \log(\|y\|_p), \dots).$$

**Encadré 2**

**ENDOMORPHISMES DE L'ESPACE PROJECTIF**

*L'un des premiers exemples de transformation polynomiale dont la dynamique a été étudiée en détails est celui des transformations  $z \mapsto z^2 + c$  où  $c$  est un paramètre complexe. En coordonnées homogènes, on obtient une transformation polynomiale  $[x : y] \mapsto [x^2 + cy^2 : y^2]$  de la droite projective  $\mathbf{P}_{\mathbb{C}}^1$ . Plus généralement, si les  $P_i$ ,  $i = 0, 1, \dots, n$ , sont des polynômes homogènes de même degré  $d$  qui ne s'annulent pas simultanément en dehors de l'origine, la transformation  $g : [x_0 : x_1 : \dots : x_n] \mapsto [P_0 : P_1 : \dots : P_n]$  détermine une*

*transformation polynomiale de  $\mathbf{P}^n$ . On parle d'endomorphisme de degré  $d$ . Nous supposons toujours que le degré  $d$  est supérieur ou égal à 2. C'est bien sûr le cas de  $z \mapsto z^2 + c$ . Lorsque l'on itère la transformation  $g$ , on obtient une suite de transformations polynomiales de l'espace projectif,  $g, g^2 = g \circ g, \dots$ ; le degré des polynômes homogènes qui définissent  $g^k$  est alors égal à  $d^k$ . Il y a donc une croissance exponentielle des degrés par itération.*

De même, les hauteurs adaptées à une transformation polynomiale ont leurs analogues locaux :  $h_p^+, h_p^-$ . Chacune de ces fonctions de hauteur devrait être utile pour décrire la dynamique induite par la transformation polynomiale  $F$  sur les points  $p$ -adiques de la variété. Pour l'instant, seul le cas non arithmétique  $p = \infty$  a été suffisamment étudié. C'est ce que nous allons maintenant expliquer.

**HAUTEURS ET MESURE D'ENTROPIE MAXIMALE**

Sur la variété complexe où a lieu la dynamique ( $\mathbf{P}_{\mathbb{C}}^k$  ou  $S(P)_{\mathbb{C}}$ ), considérons les laplaciens de Monge-Ampère des fonctions de hauteurs adaptées à la dynamique :

$$\partial\bar{\partial}h_{\infty}^+, \quad \partial\bar{\partial}h_{\infty}^-.$$

Bien souvent,  $h_{\infty}^+$  et  $h_{\infty}^-$  ne sont pas différentiables et les laplaciens  $\partial\bar{\partial}h_{\infty}^+$  et  $\partial\bar{\partial}h_{\infty}^-$  doivent être pris au sens des distributions, ou plus précisément au sens des courants. Cependant, les hauteurs adaptées  $h_{\infty}^+$  et  $h_{\infty}^-$  sont continues et « pluri-sous-harmoniques », ce qui permet de multiplier ces distributions entre elles. Lorsque  $F = f$ , on construit ainsi une mesure de probabilité

$$\mu_f = (\partial\bar{\partial}h_{\infty}^+) \wedge (\partial\bar{\partial}h_{\infty}^-)$$

sur la surface  $S(P)_{\mathbb{C}}$  (encadré 1). Lorsque  $F = g$ , il faut prendre la puissance  $k^{eme}$  de  $\partial\bar{\partial}h_{\infty}^+$  pour définir une mesure  $\mu_g$  sur  $\mathbf{P}_{\mathbb{C}}^k$ .

Ces mesures de probabilité jouissent de propriétés dynamiques optimales. Tout d'abord,  $\mu_F$  est invariante par  $F$  : si  $A$  est un ensemble mesurable et si  $F^{-1}(A)$  désigne l'ensemble des points de  $V_{\mathbb{C}}$  dont l'image appartient à  $A$ , alors

$$\mu_F(F^{-1}(A)) = \mu_F(A).$$

En outre,  $\mu_F$  est l'unique mesure d'entropie maximale et les points périodiques de  $F$  s'équirépartissent vis-à-vis de  $\mu_F$ . La première de ces deux propriétés est fondamentale mais un peu technique et nous n'en parlerons pas. Que signifie la seconde ?

Pour tout entier  $N$ , notons  $\text{Per}_F(N)$  l'ensemble des points périodiques de  $F$  dont la période n'excède pas  $N$  et  $\nu_N$  la mesure de comptage associée à cet ensemble : par définition, si  $A$  est une partie de  $V_{\mathbb{C}}$ ,  $\nu_N(A)$  est égale à la proportion de points de  $\text{Per}_F(N)$  situés dans  $A$ . L'équirépartition des points périodiques de  $F$  vis-à-vis de  $\mu_F$  signifie que  $\nu_N$  converge vers  $\mu_F$  lorsque la taille des périodes  $N$  tend vers l'infini. Autrement dit,  $\mu_F$  décrit la répartition asymptotique des points périodiques de  $F$ .

L'histoire ne s'arrête pas là. Au lieu de regarder le système dynamique  $F : V_{\mathbb{C}} \rightarrow V_{\mathbb{C}}$  dans son ensemble, concentrons-nous sur la partie qui recèle l'essentiel de la dynamique, à savoir l'adhérence des points périodiques de  $F$ . Notons  $X_F$  ce sous-ensemble de  $V_{\mathbb{C}}$  ; il s'agit d'un espace compact invariant par  $F$  qui est muni d'une mesure de probabilité  $\mu_F$  elle aussi  $F$ -invariante. Le théorème le plus frappant obtenu actuellement affirme que le système est semblable à un jeu de pile ou face. En termes techniques, il existe un changement de variable mesurable  $m' = \Psi(m)$ , qui conjugue le triplet  $(X_F, \mu_F, F)$  à un décalage de Bernoulli : quitte à négliger les ensembles de mesure nulle pour  $\mu_F$ , la dynamique est donc aussi aléatoire qu'un jeu de pile ou face.

Tous ces résultats de nature dynamique sont le fruit d'une lente progression dont les acteurs principaux sont Eric Bedford, Jean-Yves Briend, Julien Duval, Michael Lyubich, Ricardo Mañe, Nessim Sibony, John Smillie... et bien d'autres encore !

## CONCLUSION

Historiquement, les fonctions de hauteurs adaptées  $h_{\infty}^{+}$  ne sont pas apparues au sein des systèmes dynamiques *via* leur construction arithmétique. Elles ont d'abord été introduites par des méthodes de théorie du potentiel. Les relations entre arithmétique et dynamique

que nous avons décrites dans ce texte enjolivent donc un peu l'histoire et en cachent une partie importante. Si nous avons choisi cette présentation des faits, c'est pour illustrer les liens qui existent entre deux domaines *a priori* éloignés. De nombreuses questions à la frontière de ces domaines restent actuellement sans réponse. Nous espérons que ces liens se renforceront dans les années à venir.

### POUR EN SAVOIR PLUS

**Hindry (M.), Silverman (J.-H.),** « Diophantine Geometry, an Introduction », *Springer Verlag, GTM*, 2000.

**Cerveau (D.), Ghys (É.), Sibony (N.), Yoccoz (J.-C.),** « Dynamique et géométrie complexe », *Société mathématique de France, Panoramas et synthèse*, 1999.

# Le modèle d'Ising et la coexistence des phases

**L'eau et l'huile sont constituées de molécules qui bougent au hasard.  
Or, une goutte d'huile dans l'eau est sphérique à l'équilibre, sa forme est déterministe.  
Comment le hasard présent au niveau microscopique peut-il induire de tels effets à notre échelle ?**

Commençons par décrire une simple expérience mettant en évidence le phénomène de coexistence et de séparation des phases afin de motiver nos considérations mathématiques. Le système que nous nous proposons de considérer est un mélange de deux substances : l'huile et l'eau. Rappelons que l'huile et l'eau ont tendance à se repousser cependant une petite quantité d'huile peut être parfaitement dissoute dans l'eau et *vice-versa* (le mélange de phénol et d'eau serait un choix plus réaliste car ils sont plus miscibles, le mélange d'eau et de sel est aussi un bon exemple, mais le phénomène que nous voulons décrire est plus complexe dans ce cas). Comme nous le savons, la solubilité n'est pas infinie. En fonction de la température  $T$ , il existe des seuils de densités  $d_c^{h/e}(T)$  et  $d_c^{e/h}(T)$  (tous deux croissant avec  $T$ ) correspondant respectivement aux solutions saturées d'huile dans l'eau et d'eau dans l'huile. Ces deux types de solutions saturées sont appelées les phases pures « h/e » et « e/h » et correspondent à un équilibre parfait entre l'énergie et l'entropie.

Afin d'observer la séparation des phases dans ce système, tout ce que nous avons à faire est de prendre une solution quasiment saturée d'huile dans l'eau à densité  $d$  et à température  $T$ , et de laisser le système refroidir jusqu'à une température  $T'$  telle que  $d > d_c^{h/e}(T')$ . L'excès d'huile précipite et des gouttes macroscopiques apparaissent. L'intérieur des gouttes ne contient pas de l'huile pure : les gouttes sont en réalité des régions où nous voyons la phase e/h. Les gouttes nagent dans la phase h/e (si nous supposons qu'il n'y a pas de gravité, sinon la phase e/h se concentre en haut). Quelle est la loi qui gouverne le comportement des phases qui coexistent ?

La théorie phénoménologique classique affirme qu'il existe une énergie libre de surface  $\mathcal{I}$  associée aux bords des phases macroscopiques et que le système se dirige vers un état minimisant cette énergie. Si le système est

isotrope,  $\mathcal{I}$  est proportionnelle à l'aire. Ainsi, à l'équilibre parfait, il devrait y avoir une seule goutte de la phase e/h avec une forme sphérique flottant dans la phase h/e, étant donné que, par l'inégalité isopérimétrique, c'est la configuration énergétiquement la plus favorable.

Un défi mathématique est de confirmer cette théorie en partant d'une description microscopique du système ; d'expliquer l'existence de la solubilité et la saturation, la séparation des phases à l'échelle macroscopique, et de vérifier la prédiction de l'existence d'une goutte unique avec une forme spécifique. Il s'agit là de l'un des enjeux fondamentaux de la mécanique statistique : nous voulons comprendre comment le hasard qui est présent au niveau atomique peut induire des effets géométriques déterministes à notre échelle.

Essayons de construire un modèle simple de notre système. Un choix commode est d'utiliser un modèle bâti sur un réseau. Considérons donc une boîte carrée  $\Lambda(n)$  de côté  $n$  ( $n$  est très grand, de l'ordre du nombre d'Avogadro) sur le réseau des entiers  $\mathbb{Z}^2$ . Chaque site du réseau est occupé soit par une particule d'eau soit par une particule d'huile, *i.e.*, à chaque site de  $\Lambda(n)$  est associé un signe  $-$  ou  $+$  et l'état du système  $\sigma$  est décrit par l'ensemble de ces signes ; ainsi une configuration  $\sigma$  est une fonction de  $\Lambda(n)$  dans  $\{-, +\}$ . L'interaction entre les particules est répulsive et se produit lorsque les substances sont en contact immédiat. Ainsi une interaction répulsive limitée aux plus proches voisins constitue un choix raisonnable. Si nous nous intéressons seulement à l'interaction répulsive dominante entre les différentes molécules, nous pouvons simplifier le modèle en rendant les deux substances symétriques et en supposant que leurs auto-interactions sont de grandeur égale et qu'elles s'annulent globalement. Donc, l'énergie totale d'une configuration doit être simplement le nombre de toutes les paires de plus proches voisins de signes différents, ce qui donne la formule suivante

$$\forall \sigma \in \{-, +\}^{\Lambda(n)}$$
$$H(\sigma) = -\frac{1}{2} \sum_{x,y \text{ voisins}} \sigma(x)\sigma(y) + \text{constante}$$

Nous mettons ensuite du hasard dans le modèle en introduisant une température  $T$  et en définissant la probabilité  $\mu_T(\sigma)$  d'une configuration  $\sigma$  par la mesure de Gibbs

$$\forall \sigma \in \{-, +\}^{\Lambda(n)}$$

$$\mu_{\Lambda(n), T}(\sigma) = \frac{\exp\left(-\frac{H(\sigma)}{T}\right)}{\sum_{\eta \in \{-, +\}^{\Lambda(n)}} \exp\left(-\frac{H(\eta)}{T}\right)}$$

Nous venons de décrire le modèle d'Ising, sans doute le plus fameux modèle de mécanique statistique pour étudier les transitions de phase. Une configuration est d'autant plus stable que son énergie est petite, c'est-à-dire que le nombre d'interfaces entre les  $-$  et les  $+$  est petit. Les particules de même type ont donc une tendance probabiliste à se regrouper, tandis que le hasard a tendance à les faire se mélanger.

Lorsque la température  $T$  est petite, c'est l'effet de regroupement qui domine (il est très improbable d'observer des particules distinctes sur des sites voisins), tandis qu'à haute température, cet effet disparaît et toutes les particules se mélangent de manière parfaitement homogène. Mathématiquement, il est possible de prouver que lorsque la dimension du réseau est supérieure ou égale à deux, il existe une température critique  $T_c$  telle que, pour  $T < T_c$  on observe deux phases distinctes (l'une dominée par les  $-$ , l'autre par les  $+$ ) qui se séparent à l'échelle macroscopique, tandis que pour  $T > T_c$ , le système produit toujours un mélange parfaitement homogène. Ce phénomène peut également être détecté grâce à l'aimantation spontanée, définie par

$$m^* = \lim_{n \rightarrow \infty} \mu_{\Lambda(n), T}^+(\sigma(0))$$

où  $\mu_{\Lambda(n), T}^+$  est la mesure de Gibbs dans la boîte  $\Lambda(n)$  à la température  $T$  et avec conditions au bord plus, *i.e.*, la boîte est entourée par une rangée de  $+$  fixes. Ces plus influencent les particules du bord de la boîte qui elles-mêmes influencent les particules à distance 1 du bord, et l'effet voyage de la sorte jusqu'à la particule  $\sigma(0)$  au centre de la boîte. Comme l'influence de cet effet décroît avec le diamètre  $n$  de la boîte, la limite ci-dessus existe par monotonie. Lorsque  $T > T_c$ ,  $m^*$  vaut 0, tandis que lorsque  $T < T_c$ ,  $m^*$  est strictement positive : le système garde une mémoire des conditions au bord après qu'on les a envoyées à l'infini et l'information se transmet dans le système à l'échelle macroscopique. L'aimantation spontanée  $m^*$  donne l'excédent typique de densité des  $+$  dans la phase pure où les  $+$  dominent ; en effet, on a une convergence ergodique :

$\forall \varepsilon > 0$

$$\lim_{n \rightarrow \infty} \mu_{\Lambda(n), T}^+ \left( \left| \frac{1}{|\Lambda(n)|} \sum_{x \in \Lambda(n)} \sigma(x) - m^* \right| < \varepsilon \right) = 1.$$

Rappelons que dans notre expérience la densité de l'huile est fixée, donc nous avons une contrainte sur les configurations possibles : la proportion de  $+$  et de  $-$  dans la boîte  $\Lambda(n)$  doit être fixée. Nous imposons de telles conditions au modèle d'Ising dans le régime de coexistence de phases  $T < T_c$  et nous voulons comprendre et décrire mathématiquement les configurations les plus probables du système. Ce programme a été conduit avec succès en dimension 2 il y a environ dix ans par Dobrushin, Kotecký et Shlosman. Il existe dans le cas du modèle d'Ising une difficulté supplémentaire par rapport à notre expérience, qui est due à l'utilisation du réseau : le modèle est anisotrope et l'énergie de surface dépend de la direction. Les gouttes correspondantes ne sont pas sphériques, ce sont des patatoïdes convexes qui sont appelés gouttes de Wulff ou cristal de Wulff, celui-ci étant le premier à avoir étudié et résolu le problème isopérimétrique correspondant, il y a un siècle.

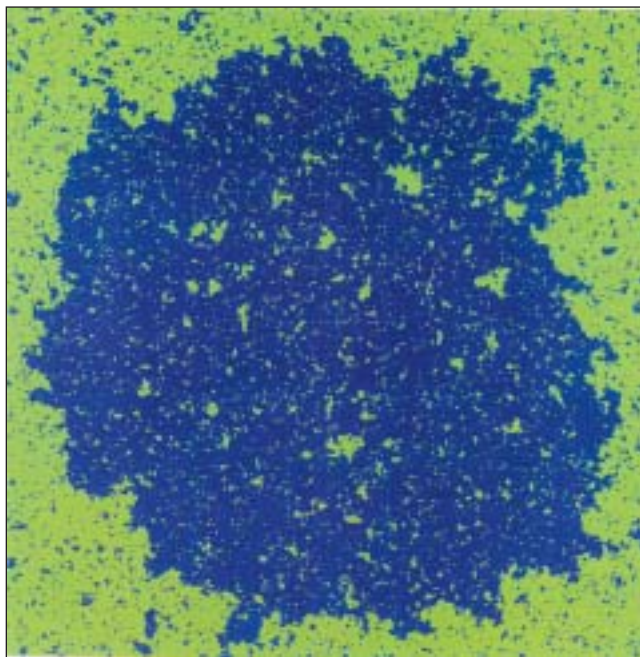


Figure 1 - Une goutte dans le modèle d'Ising en dimension 2.

Récemment, l'étude a été menée en dimension 3 et plus par Bodineau, Cerf et Pisztora. Plusieurs problèmes doivent être surmontés pour attaquer le cas de la dimension 3. Tout d'abord, la topologie de la distance de Hausdorff entre les frontières des ensembles est inadaptée. En effet dans l'espace, de longs et fins filaments augmentent de manière dramatique la distance de Hausdorff sans pour autant créer beaucoup d'énergie de surface. Le cristal de Wulff n'est donc plus une solution stable du pro-

blème isopérimétrique et il est nécessaire de reformuler le résultat. Mais l'obstacle majeur pour étendre la preuve de la dimension 2 à la dimension 3 est la technologie des squelettes, qui consiste à approximer une courbe polygonale décrivant le bord d'une goutte par une autre plus grossière et à utiliser ensuite une borne combinatoire sur le nombre de courbes polygonales. La structure des surfaces de dimension 2 est si riche par rapport à celle des courbes, qu'il semble très ardu de trouver un argument combinatoire similaire en dimension plus grande que 2. Une nouvelle stratégie est donc nécessaire. Une voie naturelle consiste à quitter le cadre discret et à essayer de travailler directement dans le continu, afin de remplacer l'argument combinatoire par un argument de compacité. Il faut donc que nos gouttes aléatoires soient plongées dans un espace continu et que les ensembles de niveau de l'énergie de surface soient compacts. Si de plus le volume est une fonctionnelle continue, alors nous aurons l'existence de solutions pour nos problèmes variationnels, un point hautement souhaitable. Tout cela rappelle la théorie probabiliste des grandes déviations : nous demandons que l'énergie de surface soit une bonne fonction de taux. Et donc, pourquoi ne pas chercher un principe de grandes déviations dans cet espace continu idéal, gouverné par l'énergie de surface ? Les résultats sur la construction de Wulff seraient alors des conséquences naturelles de ce principe de grandes déviations : sous une contrainte de volume, les gouttes aléatoires se concentrent automatiquement près des objets réalisant l'infimum de la fonction de taux. Mais dans quel espace continu travailler ?

Il est clair que cet espace doit nécessairement contenir toutes les surfaces régulières (car elles peuvent être approximées par des surfaces polygonales) et que si  $\Gamma$  est une surface régulière, alors son énergie de surface  $\mathcal{I}(\Gamma)$  doit être

$$\mathcal{I}(\Gamma) = \int_{\Gamma} \tau(v_{\Gamma}(x)) ds(x)$$

où  $v_{\Gamma}(x)$  est le vecteur normal à  $\Gamma$  en  $x$ ,  $\tau(v)$  est la tension de surface du modèle dans la direction  $v$  et  $ds$  est la mesure de surface sur  $\Gamma$ . Le problème de l'extension de telles fonctionnelles d'énergie de surface à des surfaces générales non régulières et de la définition de bonnes topologies sur les espaces de surfaces n'est pas nouveau. La littérature correspondante est très riche et c'est toujours un domaine de recherche actif. Ces questions sont reliées aux problèmes d'existence et de régularité des surfaces minimales, comme le problème de Plateau : trouver la surface d'aire minimale qui s'appuie sur une courbe donnée de l'espace. Pour autant que nous puissions en juger, le cadre le plus satisfaisant pour obtenir de bonnes propriétés de compacité est la théorie des courants et les outils de la théorie de la mesure géométrique décrits dans le livre monumental de Federer. De plus, le

théorème isopérimétrique général de Wulff a été prouvé par Taylor dans ce cadre. Ce théorème dû initialement à Wulff dit que, *modulo* les translations et les ensembles négligeables, le cristal de Wulff

$$\mathcal{W}_{\tau} = \{x \in \mathbb{R}^3 : x \cdot w \leq \tau(w) \text{ pour tout vecteur unité } w\}$$

est la seule solution du problème variationnel

$$\begin{aligned} \text{minimiser } \mathcal{I}(E) &= \int_{\partial E} \tau(v_E(x)) ds(x) \\ \text{avec volume } E &\geq \text{volume } \mathcal{W}_{\tau}. \end{aligned}$$

Cependant, il apparaît que les objets utilisés dans la preuve du théorème isopérimétrique de Wulff constituent une classe particulière de courants qui peuvent être identifiés avec les ensembles de Caccioppoli, également appelés ensembles de périmètre localement fini. Il s'agit d'une théorie géométrique différente, initiée par Caccioppoli (la figure centrale du film « Morte da un matematico napoletano » de Mario Martone) et développée par De Giorgi, qui a entre autres choses permis d'obtenir la solution générale du problème de Plateau en toutes dimensions. Cette théorie est beaucoup plus accessible. Par exemple, le théorème de Wulff a été redémontré et légèrement amélioré dans ce contexte par Fonseca. Ce cadre est le plus naturel pour analyser la géométrie des interfaces entre des phases stables qui coexistent. D'ailleurs, la théorie phénoménologique des transitions de phases est développée dans ce cadre. L'énergie de surface d'un ensemble borélien  $A$  de  $\mathbb{R}^3$  est

$$\mathcal{I}(A) = \sup \left\{ \int_A \operatorname{div} f(x) dx : f \in C_0^1(\mathbb{R}^3, \mathcal{W}_{\tau}) \right\}$$

où  $C_0^1(\mathbb{R}^3, \mathcal{W}_{\tau})$  est l'ensemble des champs de vecteurs  $C^1$  définis sur  $\mathbb{R}^3$  à support compact et à valeurs dans  $\mathcal{W}_{\tau}$ , et  $\operatorname{div}$  l'opérateur usuel de divergence. L'énergie de surface  $\mathcal{I}(A)$  est infinie sauf si  $A$  est un ensemble de périmètre fini au sens de Caccioppoli et De Giorgi. Nous évaluons d'abord la probabilité d'avoir un déficit de plus dans  $\Lambda(n)$  avec condition au bord plus. Définissons le cristal de Wulff dilaté

$$\begin{aligned} \forall m \in [-m^*, m^*] \\ \mathcal{W}(m) &= \left( \frac{m^* - m}{2m^*} \right)^{1/3} (\text{volume}(\mathcal{W}_{\tau}))^{-1/3} \mathcal{W}_{\tau}. \end{aligned}$$

Soit  $m$  tel que  $\mathcal{W}(m)$  rentre complètement dans le cube unité et soit  $T < \widehat{T}_c$  (la preuve actuelle fonctionne jusqu'à une température  $\widehat{T}_c$  qui est conjecturée coïncider avec  $T_c$ ). Alors

$$\mu_{\Lambda(n), T}^+ \left( \frac{1}{n^3} \sum_{x \in \Lambda(n)} \sigma(x) \leq m \right) \underset{n \rightarrow \infty}{\sim} \exp -n^2 \mathcal{I}(\mathcal{W}(m)).$$

Nous décrivons ensuite l'équilibre du système lorsque l'on force un excès de moins. Nous montrons qu'une seule goutte macroscopique de la phase moins émerge : cette goutte est proche du cristal de Wulff, elle est entourée par la phase plus et contient tout l'excédent de moins. Un bon moyen pour localiser la goutte est de regarder la moyenne locale sur une échelle intermédiaire. Soit  $\Gamma_n^-$  l'ensemble des points de  $\Gamma$  où celle-ci est négative :

$$\Gamma_n^- = \left\{ x \in \Gamma : \sum_{y \in \Lambda(n)} \sigma(y) 1_{|y-nx| < n^{1/3}} < 0 \right\}.$$

L'ensemble  $\Gamma_n^-$  est la zone où les moins sont localement majoritaires. Créons de force un excès de moins en conditionnant la probabilité  $\mu_{\Lambda(n), T}^+$  ; alors

$$\lim_{n \rightarrow \infty} \mu_{\Lambda(n), T}^+ \left( \exists x \in \Lambda(n) \text{ volume}(\Gamma_n^- \Delta(x + \mathcal{W}(m))) < \delta \left| \frac{1}{n^3} \sum_{x \in \Lambda(n)} \sigma(x) \leq m \right. \right) = 1.$$

Ce résultat est en fait une loi des grands nombres, que nous pourrions exprimer ainsi :

$$\lim_{\text{nombre de particules} \rightarrow \infty} \left( \begin{array}{c} \text{effet total des forces} \\ \text{microscopiques repulsives} \end{array} \right) = \text{création d'une goutte unique.}$$

L'objet limite déterministe est la forme géométrique de la goutte à l'équilibre. Il est conjecturé que le cristal de Wulff devient parfaitement sphérique lorsque  $T \rightarrow T_c$ . Ainsi la perfection géométrique peut naître du hasard...

### SIMULATIONS DU MODÈLE D'ISING

Ces images ont été réalisées grâce à **gising**, disponible via la page [www.math.u-psud.fr/~cerf](http://www.math.u-psud.fr/~cerf).

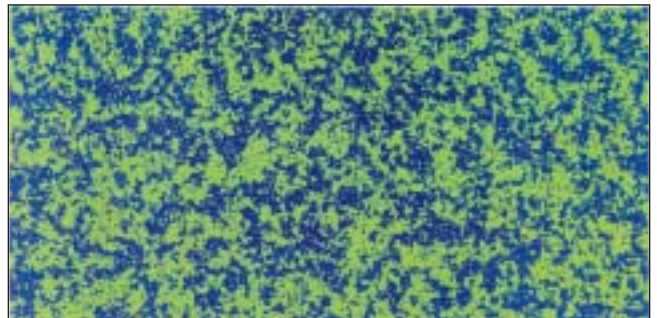


Figure 2a - Température sur-critique : une seule phase homogène.

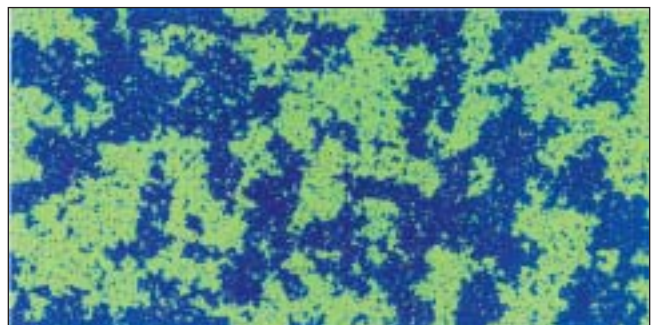


Figure 2b - Température critique : le système hésite...

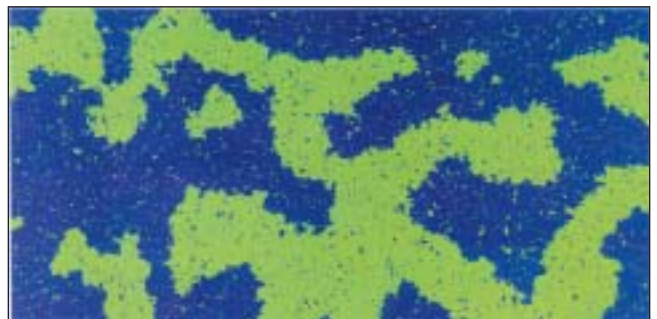


Figure 2c - Température sous-critique : les deux phases se séparent.

#### Encadré 1

## LES GRANDES DÉVIATIONS

La théorie des grandes déviations est une théorie probabiliste qui étudie les événements rares, i.e., les événements de faible probabilité. Elle propose un formalisme et des méthodes robustes qui fonctionnent dans des situations très diverses. De manière schématique, on considère un objet aléatoire  $X_n$  dépendant d'un paramètre qui, lorsque  $n$  tend vers l'infini, adopte un comportement typique. Si  $A$  est un ensemble de configurations qui n'inclut pas ce comportement typique, alors  $P(X_n \in A)$  tend vers 0 lorsque  $n$  tend vers l'infini. L'événement  $\{X_n \in A\}$  est alors un événement de grandes déviations et sa probabilité est estimée par une expression de la forme

$$P(X_n \in A) \underset{n \rightarrow \infty}{\sim} \exp -n \inf \left\{ I(x) : x \in A \right\}$$

où  $I$  est une fonctionnelle caractérisant la vitesse asymptotique de décroissance vers 0 de la probabilité, appelée fonction de taux. Le symbole  $\underset{n \rightarrow \infty}{\sim}$  signifie que les logarithmes des membres de gauche et de droite sont des infiniment grands équivalents lorsque  $n \rightarrow \infty$ . La formule précédente ramène le problème de l'estimation de  $P(X_n \in A)$  à un problème de calcul variationnel  $\inf \{ I(x) : x \in A \}$ . La théorie des grandes déviations est ainsi un pont entre les probabilités et le calcul des variations.

**Encadré 2**

**DISTANCES ENTRE ENSEMBLES**

Nous cherchons à exprimer le fait que la forme typique d'une goutte à l'équilibre est décrite par le cristal de Wulff. Pour cela, il est nécessaire de mesurer la distance entre deux formes et donc d'introduire une métrique sur l'espace des ensembles. En dimension 2, la distance de Hausdorff est très bien adaptée. Si  $A, B$  sont deux parties de  $\mathbb{R}^2$ , la distance de Hausdorff  $d(A, B)$  entre  $A$  et  $B$  est définie par

$$d(A, B) = \max \left\{ \sup_{a \in A} \inf_{b \in B} |a - b|, \sup_{b \in B} \inf_{a \in A} |b - a| \right\}.$$

Si nous nous restreignons à la collection des parties compactes de  $[0, 1]^2$ , alors  $d$  vérifie tous les axiomes d'une distance classique. Cette distance n'est pas adéquate pour la dimension 3, car elle est trop sensible à la présence de filaments, qui augmentent énormément la distance sans créer

pour autant de surface ou de volume. Nous utilisons alors comme distance le volume de la différence symétrique : si  $A, B$  sont deux parties boréliennes de  $\mathbb{R}^3$ , la distance  $d(A, B)$  entre  $A$  et  $B$  est définie par

$$d(A, B) = \text{volume}(A \Delta B),$$

où  $\text{volume}(\cdot)$  est la mesure de Lebesgue dans  $\mathbb{R}^3$  et  $\Delta$  la différence symétrique ensembliste :

$$A \Delta B = (A \setminus B) \cup (B \setminus A).$$

Deux ensembles qui diffèrent d'un ensemble de mesure de Lebesgue nulle sont alors indistinguables et, à part ce détail, tous les axiomes classiques sont vérifiés par cette distance.

**POUR EN SAVOIR PLUS**

**Bodineau (T.)**, *The Wulff construction in three and more dimensions.*, Commun. Math. Phys., **207**, 197-229, 1999.  
**Cerf (R.), Pisztor (A.)**, *On the Wulff crystal in the Ising model*, Ann. Probab., **28 n° 3**, 947-1017, 2000.  
**Dobrushin (R.-L.), Kotecky (R.), Shlosman (S.-B.)**, *Wulff construction: a global shape from local interaction*, AMS translations series, Providence (Rhode Island), 1992.



# Mouvements browniens fractionnaires et multifractionnaires

**L'étude de phénomènes irréguliers a pris une place très importante dans beaucoup de domaines scientifiques : mécanique des fluides, traitement de l'image, mathématiques financières. Les spécialistes de ces domaines s'adressent souvent aux mathématiciens pour leur fournir des modèles permettant des calculs simples et qui soient proches des expériences. On montrera dans cet article comment l'autosimilarité sert à générer des modèles efficaces. Par ailleurs, l'utilisation de fonctions aléatoires est un outil pratique pour obtenir des exemples génériques. A l'intersection de ces deux techniques se trouvent les processus fractionnaires. Nous illustrerons notre propos grâce à deux exemples célèbres : les mouvements browniens fractionnaires et multifractionnaires. Pour conclure, nous présenterons les méthodes statistiques qui permettent aux praticiens de passer des données expérimentales aux processus mathématiques.**

De plus en plus d'applications exigent des mathématiciens de comprendre des phénomènes irréguliers. On peut citer notamment l'étude de flots turbulents où des tourbillons concentrent une grande partie de l'énergie du système, l'évolution du cours d'une action en bourse ou encore la surface très rugueuse d'un objet catalytique dans une réaction chimique. Face à ces problèmes, les mathématiciens doivent souvent abandonner des modèles fondés sur la linéarisation ou, plus généralement, le calcul différentiel classique. Dans un cadre déterministe, un des outils fondamentaux est la notion de fractale popularisée par Mandelbrot. Dans une fractale, un motif élémentaire est répété à chaque échelle par un procédé récurrent. L'étude de ces objets est facilitée par leur autosimilarité : si l'on prend une loupe ou si on les regarde de très loin, ils ont toujours la même structure. L'autosimilarité, comme toutes les propriétés d'invariance, a beaucoup de vertus pour le mathématicien, c'est ce qui permet l'analyse de ces objets souvent très complexes. Cependant, on peut se demander pourquoi l'autosimilarité génère de l'irrégularité. Tout d'abord il est facile de construire des exemples où ce n'est pas le cas, lorsque le motif initial est constant par exemple. En dehors de ces cas particuliers inintéressants, la moindre variation dans le motif initial se propage à toutes les échelles pour produire un résultat très irrégulier.

## IRRÉGULARITÉ HÖLDÉRIENNE

Par ailleurs, un vaste problème est de quantifier l'irrégularité d'un phénomène de manière à la fois précise et efficace. Pour simplifier cette présentation je restreindrai cette étude aux fonctions qui partent d'un cube et à valeurs dans l'ensemble  $\mathbb{R}$  des réels  $f : [0, 1]^d \rightarrow \mathbb{R}$ . Une manière de décrire à quel point une fonction varie brutalement est de comparer ses variations à celles d'une puissance fractionnaire de la norme euclidienne. Par exemple si  $\forall x, y \in [0, 1]^d |f(x) - f(y)| \leq C \|x - y\|^H$  pour  $C$  une constante finie, on dit que  $f$  est  $H$ -höldérienne. Comme les fonctions puissances sont bornées sur le cube, il suffit de vérifier l'inégalité pour  $x$  proche de  $y$  et l'on constate ainsi que si  $f$  est  $H$ -höldérienne, elle est  $H'$ -höldérienne pour tout  $0 < H' < H$ . Ce qui importe donc pour mesurer l'irrégularité d'une fonction, c'est le plus grand  $H$  telle que  $f$  est  $H$ -höldérienne. De plus, cette notion peut être localisée en un point  $x$  et l'on définit alors l'exposant de Hölder ponctuel  $H(f, x)$  :

$$H(f, x) = \sup_{H'} \left\{ \lim_{\varepsilon \rightarrow 0} \frac{f(x + \varepsilon) - f(x)}{\varepsilon^{H'}} = 0 \right\}. \quad (1)$$

En fait, on ne considère que des exposants  $H < 1$  car pour  $H$  égal à 1 la fonction  $f$  est régulière et notamment

**Encadré 1**

**L'AUTOSIMILARITÉ ENTRAÎNE DE L'IRRÉGULARITÉ :  
COURBE DE VON KOCH**

**Figure 1** - Courbe de Von Koch : état initial.



**Figure 3** - Courbe de Von Koch : étape 2.



**Figure 2** - Courbe de Von Koch : motif, étape 1.



**Figure 4** - Courbe de Von Koch : étape 3.



*Dans les figures ci-dessus on remarque que le motif triangulaire qui est introduit à l'étape 1 rend de plus en plus irrégulière la fonction initialement constante.*

toutes les fonctions continûment dérivables sont 1-hölderiennes. Une autre manière de quantifier l'irrégularité d'une fonction est de mesurer la dimension de Hausdorff du graphe

$$G_f = \{(x, f(x)) \mid 0 \leq x \leq 1\}.$$

La dimension de Hausdorff que nous noterons  $\dim_{Ha} G_f$  est comprise entre 1 et 2. Si  $f$  est continûment dérivable  $\dim_{Ha} G_f = 1$  et on retrouve le graphe d'une courbe lisse qui est de dimension 1. En revanche, dès que  $\dim_{Ha} G_f > 1$ ,  $G_f$  est une vraie fractale. Rappelons que si  $f$  est  $H$ -höldérienne  $\dim_{Ha} G_f \leq 2 - H$ .

**AUTOSIMILARITÉ STATISTIQUE**

Même si les fractales et l'autosimilarité sont des substituts efficaces à la linéarité pour étudier l'irrégularité, il n'en demeure pas moins que beaucoup des questions posées aux mathématiciens par les non-mathématiciens ne sont pas résolues. On peut citer par exemple le calcul de la dimension de Hausdorff du graphe de la fonction de Weierstrass qui n'est pas rigoureusement établi à ce jour.

De plus, les expérimentateurs cherchent souvent à disposer de modèles leur fournissant des ensembles de fonctions génériques qu'ils pourront mieux comparer à leurs

observations qu'un exemple particulier de fonction. Toutes ces raisons expliquent sans doute la popularité des modèles où l'irrégularité se conjugue avec l'aléa. On fait alors appel au probabiliste pour construire des processus (fonctions dépendant du hasard) tels que l'on puisse spécifier leur irrégularité sans pour autant pouvoir prédire la forme particulière de la fonction générée. Pour illustrer cette manière de penser, prenons l'exemple du mouvement brownien fractionnaire  $(B_H(x, \omega))_{x \in [0,1]}$  introduit en 1939 par Kolmogorov, où  $\omega$  est l'aléa. Le mouvement brownien fractionnaire est un processus gaussien, ce qui simplifie considérablement la description de sa loi. En effet pour les processus gaussiens  $G$ , il suffit de spécifier la moyenne des valeurs de la fonction appelée espérance et notée  $\mathbb{E}G(x)$  et la dispersion de ces valeurs par rapport à la moyenne mesurée par l'écart type  $(\mathbb{E}[G(x) - \mathbb{E}G(x)]^2)^{1/2}$  pour caractériser complètement le modèle. Dans le cas du mouvement brownien fractionnaire, le processus est d'espérance nulle, *i.e.* pour tout  $x$ ,  $\mathbb{E}B_H(x) = 0$  et  $B_H(0) = 0$ . En fait, ce sont les variations du processus qui nous intéressent. Ces dernières sont contrôlées par la dispersion des accroissements

$$(\mathbb{E}(B_H(x) - B_H(y))^2)^{1/2} = \|x - y\|^H. \quad (2)$$

On peut interpréter (2) en disant que le mouvement brownien fractionnaire est  $H$ -hölderien pour l'écart type.

Si  $H = 1/2$ , l'équation (2) se simplifie ; on parle alors de mouvement brownien standard. Ce cas particulier  $H = 1/2$  a beaucoup de propriétés supplémentaires par rapport au cas général  $H \neq 1/2$  mais comme notre propos est de faire varier  $H$  nous n'en discuterons pas dans cet article. Il nous faut maintenant expliquer le lien entre le mouvement brownien fractionnaire et l'autosimilarité. Bien que pour un aléa fixé  $\omega$ , les trajectoires  $x \rightarrow B_H(x, \omega)$  ne soient pas fractales, nous retrouvons la propriété d'autosimilarité en moyenne

$$B_H(\varepsilon x) \stackrel{\mathcal{L}}{=} \varepsilon^H B_H(x). \quad (3)$$

L'égalité au sens des lois des processus notée  $\stackrel{\mathcal{L}}{=}$  signifie que quand on fait des moyennes en prenant un grand nombre de trajectoires à gauche et à droite du signe égal,

## VERS LE MULTIFRACTIONNAIRE

Le mouvement brownien fractionnaire est un sujet d'étude en soi passionnant mais du point de vue des applications à la modélisation des phénomènes rugueux, c'est un modèle trop pauvre. Expliquons cela à partir d'un exemple d'école tiré du traitement de l'image. Dans ce domaine, les trajectoires du mouvement brownien fractionnaire ont été utilisées pour simuler le profil d'un massif montagneux. Si l'on se reporte à l'encadré 2, la figure où  $H = 0,8$  semble convenir pour un massif plus ancien que celle pour  $H = 0,6$ . Plus le massif est ancien, plus les profils des montagnes sont réguliers. Si l'on raffine cette démarche on peut se souvenir que plus la roche du sol est dure, plus le massif est escarpé et plus grande sera l'irrégularité de la trajectoire. Dans ce cas, on auto-

### Encadré 2

## SIMULATION DE TRAJECTOIRES DU MOUVEMENT BROWNIEN FRACTIONNAIRE

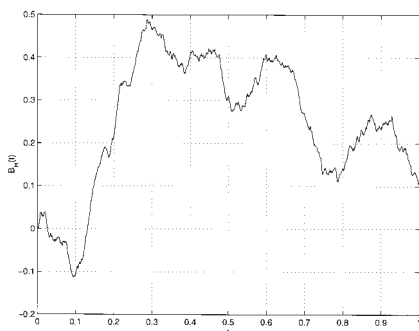


Figure 1 - Trajectoire pour  $H = 0.8$ .

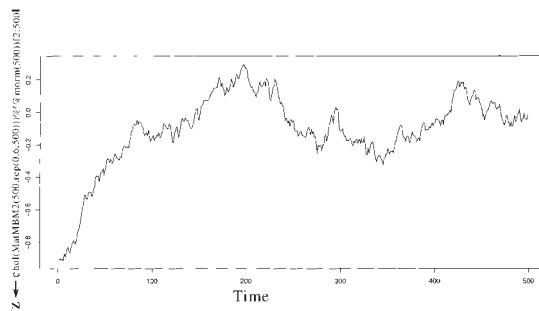


Figure 2 - Trajectoire pour  $H = 0.6$ .

on obtient des résultats identiques. En ce qui concerne l'irrégularité des trajectoires du mouvement brownien fractionnaire, le résultat est encore plus satisfaisant : en tout point  $x \in [0, 1]$ , en dehors d'un ensemble de trajectoires qui est de probabilité nulle, l'exposant de Hölder ponctuel du mouvement brownien fractionnaire ne dépend pas du hasard et est égal à  $H$  :

$$H(B_H, x) = H \quad \text{p.s.} \quad (4)$$

De plus  $\dim_{H^a} G_{B_H} = 2 - H$  p.s. Il faut noter que nous donnons ici dans un souci de simplification une version particulièrement faible des résultats connus sur la régularité des trajectoires du mouvement brownien fractionnaire.

rise le paramètre  $H$  à dépendre de la position du point  $x$ . En fait, la fonction  $x \rightarrow H(x)$  est souvent la fonction d'intérêt car elle traduit la nature géologique du sous-sol. Cependant, quand on revient à la présentation mathématique du mouvement brownien fractionnaire, on s'aperçoit que  $H$  ne peut pas varier. Dans (4), l'exposant de Hölder ponctuel est presque sûrement constant. Plus grave, l'autosimilarité (3) est une propriété d'invariance qui concerne l'ensemble de la trajectoire. Des raisons plus profondes issues notamment de l'étude de la turbulence ont conduit un certain nombre d'auteurs à proposer une généralisation du mouvement brownien fractionnaire : le mouvement brownien multifractionnaire. Pour construire le mouvement brownien multifractionnaire, nous devons

Encadré 3

## SIMULATION DE TRAJECTOIRES DU MOUVEMENT BROWNIEN MULTIFRACTIONNAIRE

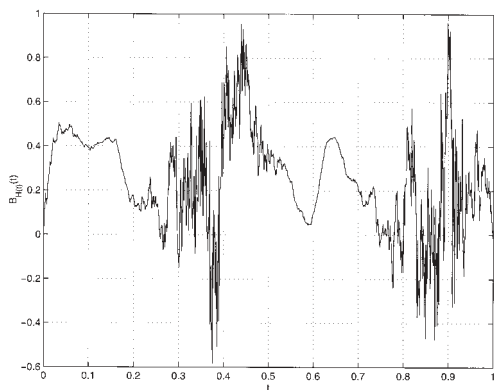


Figure 1 - Trajectoire d'un brownien multifractionnaire.

Dans la figure ci-contre, la fonction multifractionnaire  $x \rightarrow h(x)$  est périodique. Elle est petite pour  $x$  proche de 0, atteint un maximum en 0,4 et en 0,9. On peut suivre ses modulations sur l'irrégularité de la trajectoire du mouvement brownien multifractionnaire associé.

revenir sur la représentation spectrale du mouvement brownien fractionnaire. En tant que processus gaussien à accroissements stationnaires, le mouvement brownien fractionnaire admet une densité spectrale  $f(\lambda)$  qui représente d'un point de vue physique la répartition de l'énergie dans les différentes fréquences notées ici  $\lambda$ . Or, la propriété d'autosimilarité (3) se traduit sur la densité spectrale par une propriété d'homogénéité et la relation (2) fixe le degré d'homogénéité ; on en déduit que

$$f(\lambda) = \frac{C_H}{|\lambda|^{H+1/2}}, \quad (5)$$

et une représentation de type Fourier du mouvement brownien fractionnaire

$$B_H(x) = \int_{\mathbb{R}} \frac{e^{-ix\lambda} - 1}{C_H \|\lambda\|^{H+1/2}} \widehat{W}(d\lambda), \quad (6)$$

appelée représentation harmonisable du mouvement brownien fractionnaire. Dans la formule (6), on reconnaît avec le terme  $e^{-ix\lambda}$  une transformation de Fourier inverse où le  $-1$  du numérateur assure que  $B_H(0) = 0$ . La mesure  $\widehat{W}$  est un bruit blanc gaussien tel que si  $\phi(\lambda)$  est de carré intégrable  $\int_{\mathbb{R}} \phi(\lambda) \widehat{W}(d\lambda)$  est une variable aléatoire gaussienne d'espérance nulle et de variance  $\int_{\mathbb{R}} \phi^2(\lambda) d\lambda$ . Si l'on se donne une fonction

$h : [0, 1] \rightarrow ]0, 1[$  le processus défini par sa représentation harmonisable :

$$B_h(x) = \int_{\mathbb{R}} \frac{e^{-ix\lambda} - 1}{\|\lambda\|^{h(x)+1/2}} \widehat{W}(d\lambda), \quad (7)$$

est appelé mouvement brownien multifractionnaire de fonction multifractionnaire  $h$ . Ce processus est un bon modèle pour notre exemple de profil de montagne où l'on souhaite prescrire par avance la dureté de la roche au moyen de la fonction  $h$ . En effet, on peut montrer sous des hypothèses de régularité minimale sur  $h$  que l'exposant de Hölder ponctuel du mouvement brownien multifractionnaire est presque sûrement égal à  $h(x)$  et que la dimension de Hausdorff du graphe des trajectoires du mouvement brownien multifractionnaire est

$$2 - \inf\{h(x), 0 \leq x \leq 1\}.$$

De plus, ce processus admet en chaque point  $x_0$  un mouvement brownien fractionnaire tangent au sens de la limite suivante :

$$\lim_{\varepsilon \rightarrow 0^+} \left( \frac{B_h(x_0 + \varepsilon u) - X(x_0)}{\varepsilon^{h(x_0)}} \right)_{u \in \mathbb{R}} \stackrel{\mathcal{L}}{=} a(x_0) (B_H(u))_{u \in \mathbb{R}^d} \quad (8)$$

où  $B_H$  est un brownien fractionnaire de paramètre  $H = h(x_0)$ . Dans la limite (8), on aurait un processus tangent au sens classique du terme si on divisait par  $\varepsilon$ . Cette dernière propriété, que le mouvement brownien multifractionnaire partage avec bien d'autres modèles, est appelée propriété d'autosimilarité locale asymptotique et donne l'acronyme (*lass*) en anglais. C'est une généralisation satisfaisante de la propriété d'autosimilarité (3). En effet, il est facile de vérifier qu'un mouvement brownien fractionnaire est localement autosimilaire de fonction multifractionnaire constante égale à son ordre. Dans le cas de  $B_H$  :

$$B_H(x + \varepsilon u) - B_H(x) \stackrel{\mathcal{L}}{=} B_H(\varepsilon u)$$

à cause de la propriété de stationnarité des accroissements, et l'on constate en appliquant (3) que pour un mouvement brownien fractionnaire le terme

$$\frac{B_H(x + \varepsilon u) - B_H(x)}{\varepsilon^H}$$

est constant en loi. Cette vérification élémentaire explique le dénominateur de (8) ainsi que le rôle de localisation de l'asymptotique  $\varepsilon \rightarrow 0^+$ .

#### STATISTIQUE : IDENTIFICATION DES MODÈLES

Nous avons insisté jusqu'à présent sur la construction des modèles fractionnaires et sur les propriétés probabilistes que l'on pouvait attendre de tels processus. Il est aussi essentiel pour les praticiens de pouvoir calibrer leur modèle au vue des données expérimentales. C'est typiquement un problème d'identification statistique. Précisons les contraintes de cette identification. Dans bien des cas, on ne dispose que d'un échantillon fini des valeurs du processus que l'on suppose multifractionnaire et l'on aimerait en déduire une estimation de la fonction multifractionnaire  $h$  qui apparaît dans (8). En fait, tous ces modèles possèdent des trajectoires de régularité hœlderienne ; c'est ce qui nous guidera pour bâtir des estimateurs. Dans cette optique, on remarque que l'introduction de variations de la forme :

$$V_N = \sum_{p=0}^{N-1} \left( X \left( \frac{p+1}{N} \right) - X \left( \frac{p}{N} \right) \right)^2, \quad (9)$$

pour quantifier l'irrégularité des trajectoires de  $X$  est naturelle. Esquissons un exemple d'utilisation de cette méthode dans le cas le plus simple : l'identification de l'ordre d'un mouvement brownien fractionnaire. En se souvenant que les trajectoires de nos processus sont à peu près  $C^H$  hœlderiennes, nous déduisons de (9) que

$$V_N \approx N^{1-2H} \left\{ \frac{1}{N} \sum_{p=0}^{N-2} C \left( \frac{p}{N}, \omega \right) \right\} \quad (10)$$

où  $C \left( \frac{p}{N}, \omega \right)$  représente la constante de Hölder aléatoire associée à la trajectoire  $B_H$  au point  $\frac{p}{N}$ . Par ailleurs, on voudrait appliquer une loi des grands nombres aux termes entre accolades dans (10). Or, les variables aléatoires  $C \left( \frac{p}{N}, \omega \right)$  ne sont pas en général indépendantes, et seule la propriété de décorrélation asymptotique des accroissements du mouvement brownien fractionnaire permet l'utilisation d'un principe du type « loi des grands nombres ». La formule (10) explique l'expression de l'estimateur de  $H$

$$\hat{H}_N = \frac{1}{2} \left( \log_2 \frac{V_{N/2}}{V_N} + 1 \right). \quad (11)$$

Pour obtenir des majorations de la vitesse de convergence des estimateurs en fonction du pas de discrétisation  $\frac{1}{N}$  nous souhaiterions utiliser le théorème de la limite centrale portant sur le terme entre accolades de (10). Or, il est connu que pour  $H > 3/4$  il n'existe pas de théorème de la limite centrale pour  $V_N$ . Nous trouvons à ce niveau de notre raisonnement ce qui impose de choisir une variation quadratique généralisée :

$$\tilde{V}_N = \sum_{p=0}^{N-2} \left( B_H \left( \frac{p+2}{N} \right) - 2B_H \left( \frac{p+1}{N} \right) + B_H \left( \frac{p}{N} \right) \right)^2$$

et non une variation quadratique classique  $V_N$ . On peut alors établir des vitesses de convergence en  $N^{-1/2}$  pour l'estimateur :

$$\tilde{H}_N = \frac{1}{2} \left( \log_2 \frac{\tilde{V}_{N/2}}{\tilde{V}_N} + 1 \right). \quad (12)$$

Pour le modèle du brownien multifractionnaire, il faut estimer la fonction multifractionnaire  $h$  qui définit le modèle dans (7). Le principe consiste à localiser la variation quadratique généralisée  $\tilde{V}_N$  au voisinage du point  $0 \leq x_0 \leq 1$  si l'on cherche à estimer  $h(x_0)$ . Définissons le voisinage de  $x_0$  par

$$\mathcal{V}_{\varepsilon, N}(x_0) = \left\{ p \in \mathbb{Z}, \left| \frac{p}{N} - x_0 \right| \leq \varepsilon \right\}$$

et posons comme variation quadratique généralisée :

$$\mathbf{V}_{\varepsilon, N}(x_0) = \sum_{p \in \mathcal{V}_{\varepsilon, N}(x_0)} \left( B_h \left( \frac{p+1}{N} \right) - 2B_h \left( \frac{p}{N} \right) + B_h \left( \frac{p-1}{N} \right) \right)^2,$$

nous obtenons comme estimateur au point  $x_0$  de  $h$

$$h_{\varepsilon,N}(x_0) = \frac{1}{2} \left( \log_2 \frac{\mathbf{V}_{\varepsilon,N/2}(x_0)}{\mathbf{V}_{\varepsilon,N}(x_0)} + 1 \right).$$

### PERSPECTIVES ET CONCLUSIONS

Nous avons voulu donner dans cet article un aperçu des problèmes qui se posent aux mathématiciens dans le

domaine de l'étude des phénomènes irréguliers quand ils sont modélisés par des processus fractionnaires. Les chercheurs essayent actuellement d'étendre ces techniques à des processus pour lesquels la fonction multifractionnaire elle-même est très irrégulière. Il serait par ailleurs souhaitable d'avoir des modèles où l'aléa n'est pas gaussien, car l'on sait que cette hypothèse n'est pas réaliste dans certains problèmes d'images. Ces problèmes sont l'objet de recherches en cours.

### POUR EN SAVOIR PLUS

**Benassi (A.), Cohen (S.), Istas (J.),** Processus fractionnaires : modèles et identification. *Matapli*, à paraître, 2003.

**Abry (P.), Gonçalves (P.), Lévy-Véhel (J.),** Lois d'échelles, fractales et ondelettes ; vol 1, *Hermès*, 2002.

**Abry (P.), Gonçalves (P.), Lévy-Véhel (J.),** Lois d'échelles, fractales et ondelettes ; vol 2, *Hermès*, 2002.

# Les mathématiques appliquées au cœur de la finance

**Au cours des trois dernières décennies, les outils mathématiques sont devenus déterminants en finance. Ils ont initialement contribué avec Black-Scholes à l'explosion des activités de marché et, aujourd'hui, la demande en profils hautement techniques reste importante, malgré les crises financières. Nous dressons un portrait succinct des connexions entre finance et mathématiques appliquées.**

Depuis une trentaine d'année, le paysage financier a été profondément modifié par l'apparition de marchés et produits nouveaux. Ce bouleversement fait suite à une volonté accrue de déréglementation dans les années 1970, rendant volatiles les taux d'intérêt et instables les taux de change. Des marchés organisés ont alors vu le jour et permis à des intervenants comme les entreprises industrielles et commerciales, les compagnies d'assurance et les banques d'intervenir massivement sur un marché unique et liquide. A la suite du premier de ces marchés à Chicago en 1973, la France a emboîté le pas, en créant le MATIF en 1985 (marché à terme international de France) puis le MONEP en 1987 (marché des options négociables). Le développement spectaculaire de ces activités a été rendu possible grâce aux progrès technologiques, mais aussi grâce aux outils théoriques qui ont permis de valoriser les nouveaux produits financiers. Aujourd'hui, les ingénieurs des départements de recherche et développement des institutions financières manipulent au quotidien une large palette d'outils des mathématiques appliquées : nous en proposons un rapide survol, en partant des probabilités (mouvement brownien, calcul stochastique, méthodes de simulation de type Monte-Carlo...) pour aller vers la statistique (estimations de paramètres...), tout en passant par l'analyse numérique (équations aux dérivées partielles linéaires ou non linéaires et leur résolution numérique, problèmes inverses...).

## APPROCHE PAR GESTION DYNAMIQUE DE PORTEFEUILLE

L'option d'achat (ou *Call*) est l'un des produits financiers les plus utilisés : à travers cet exemple simple, nous allons dégager les messages fondamentaux de la finance

---

– Emmanuel Gobet, Centre de mathématiques appliquées – UMR 7641 CNRS – École polytechnique, 91128 Palaiseau cedex  
tél. 01 69 33 45 63, emmanuel.gobet@polytechnique.fr

de marché. Tout d'abord, ce contrat confère à son acheteur le droit (mais pas l'obligation) d'acheter un actif risqué à un cours  $K$  fixé à la signature du contrat ( $K$  est appelé *prix d'exercice*), à la date future  $T$  appelé *échéance*. L'actif risqué peut être une action, une obligation, un taux de change ou encore une matière première... Notons  $S_t$  son cours à l'instant  $t$ . L'acheteur du contrat aura un gain en  $T$  égal à  $(S_T - K)_+$  (où  $x_+$  désigne la partie positive de  $x$ ) : en échange, il versera aujourd'hui une prime  $C_0$  au vendeur de l'option.

Pour déterminer le montant de cette prime, Black et Scholes d'une part, Merton d'autre part, jettent en 1973 les bases modernes de l'évaluation d'instruments financiers, en s'appuyant sur une gestion dynamique de portefeuille. Précisément, le vendeur de l'option va rechercher une stratégie qui, partant d'une richesse initiale  $C_0$ , lui permettra d'atteindre la richesse terminale souhaitée  $(S_T(\omega) - K)_+$  à la date  $T$ , de manière à honorer son engagement envers l'acheteur, et cela dans tous les scénarios  $\omega$  d'évolution du marché. Nous allons voir qu'il existe une solution unique à ce problème de *cible aléatoire*, explicite et de surcroît facile à calculer : ce *miracle* a été le détonateur de l'explosion des marchés d'options.

Notons  $V_t$  la valeur de ce portefeuille dynamique, investi d'une part en actifs risqués (en nombre  $\delta_t$ , soit pour un montant  $\delta_t S_t$ ) et d'autre part en placement sans risque (rémunération au taux d'intérêt  $r_t$  supposé déterministe pour simplifier, soit pour un montant  $V_t - \delta_t S_t$ ). Lorsque l'on traduit que les variations de la valeur du portefeuille sont uniquement dues à celles des actifs (autrement dit, sont exclus l'apport extérieur d'argent ou une consommation), on obtient une première équation, dite d'*autofinancement*, décrivant la variation infinitésimale de la valeur du portefeuille :

$$dV_t = r_t(V_t - \delta_t S_t)dt + \delta_t dS_t, \quad (1)$$

avec  $V_0 = C_0$ . Ainsi, pour valoriser l'option d'achat, il s'agit de trouver le coût initial  $V_0$  et la stratégie  $\delta_t$ , qui permettent d'obtenir  $V_T(\omega) = (S_T(\omega) - K)_+$  dans tous les scénarios de marché.

**MODÉLISATION A L'AIDE DU MOUVEMENT BROWNIEN**

Pour aller au bout du raisonnement, la modélisation stochastique de l'actif risqué doit être précisée. Pour cela, il est naturel de décomposer le rendement instantané  $\frac{dS_t}{S_t}$  de l'actif comme la superposition d'une tendance locale  $\mu_t dt$  et d'un bruit. Samuelson (1960), puis Black, Scholes et Merton (1973) proposent une modélisation de ce dernier à l'aide d'un mouvement brownien  $W_t$ , ce qui conduit à une dynamique *infinitésimale* du type

$$\frac{dS_t}{S_t} = \mu_t dt + \sigma(t, S_t) dW_t. \quad (2)$$

L'amplitude locale du bruit est donnée par la fonction  $\sigma(t, x) > 0$ , appelée *volatilité* : elle joue un rôle fondamental comme nous le verrons par la suite. Donner un sens rigoureux au terme de droite de l'équation (2) n'est pas simple : le premier terme est une intégrale de Lebesgue-Stieljes, mais le second est de nature différente car  $W_t$  n'est pas à variation bornée. Notons qu'en revanche, il est à variation quadratique finie : les sommes

$\sum_i (W_{t_{i+1}} - W_{t_i})^2$  convergent vers  $t$  pour un pas de subdivision de l'intervalle  $[0, t]$  tendant vers 0.

C'est le calcul stochastique dit d'Itô, qui donne un sens précis au terme de la forme  $\int_0^t h_s dW_s$ , appelée intégrale d'Itô, pour  $(h_s)_{s \geq 0}$  non anticipatif. Brièvement, cette intégrale se construit comme une limite appropriée de somme de Riemann non anticipative  $\sum_i h_{t_i} (W_{t_{i+1}} - W_{t_i})$  lorsque le pas de la subdivision tend vers 0. Considérer des intégrands non anticipatifs est assez naturel en finance, puisque cela revient à supposer que la valeur d'une stratégie de gestion à l'instant  $s$  ne dépend que de l'information disponible à l'instant  $s$ . On peut aussi développer un calcul différentiel. La formule d'Itô y joue un rôle central :

$$d[u(t, S_t)] = \partial_t u(t, S_t) dt + \partial_x u(t, S_t) dS_t + \frac{1}{2} \sigma^2(t, S_t) S_t^2 \partial_{x,x}^2 u(t, S_t) dt, \quad (3)$$

le terme de dérivée seconde supplémentaire provenant de la variation quadratique finie du mouvement brownien.

**Encadré 1**

**MOUVEMENT BROWNIEN**

**DÉFINITION**

Le mouvement brownien est un processus gaussien, à accroissements indépendants, stationnaires : son accroissement  $W_t - W_s$  ( $0 \leq s < t$ ) suit une loi gaussienne centrée, de variance  $(t - s)$ .

**BREF HISTORIQUE**

C'est en 1827 que le mouvement brownien est associé par Robert Brown aux trajectoires non différentiables de fines

particules dans un fluide ; en 1900, Louis Bachelier l'utilise le premier pour modéliser la dynamique des cours de la bourse, puis Einstein en 1905, pour décrire une particule qui diffuse. Ce n'est qu'en 1923 que Wiener formalise sa construction et c'est le début d'une activité de recherche intense, continuant de nos jours. Pour une introduction plus complète, nous renvoyons à Kahane (1994).

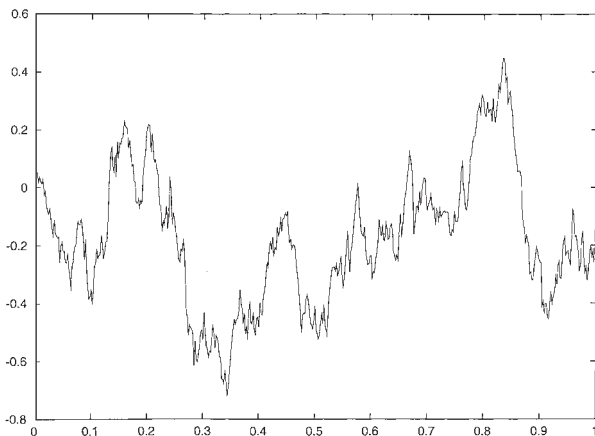


Figure 1 - Simulation d'une trajectoire brownienne.

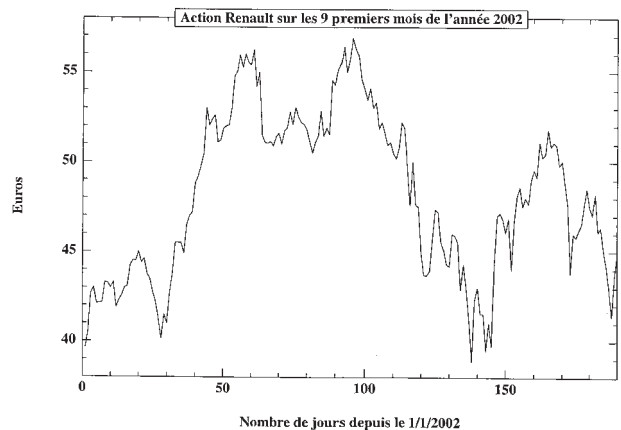


Figure 2 - Action Renault : des similarités avec le brownien...



## BLACK-SCHOLES ET LA GESTION PARFAITE

Revenons au problème de la valorisation de l'option d'achat et cherchons la valeur d'un portefeuille autofinçant sous la forme  $V_t = u(t, S_t)$  pour une certaine fonction  $u$  à déterminer. Comparons les deux écritures  $dV_t$  et  $d[u(t, S_t)]$  données par (1) et (3) en identifiant les termes en  $dt$  et  $dS_t$  : il en découle que d'une part la stratégie vaut  $\delta_t = \partial_x u(t, S_t)$  et que d'autre part,  $u$  doit nécessairement satisfaire l'équation aux dérivées partielles

$$\partial_t u + Lu - r_t u = 0, \quad (4)$$

où  $L$  est l'opérateur linéaire du second ordre défini par  $Lu(t, x) = r_t x \partial_x u(t, x) + \frac{1}{2} \sigma^2(t, x) x^2 \partial_{x,x}^2 u(t, x)$ , avec pour condition terminale  $u(T, x) = (x - K)_+$ . Remarquons que la tendance locale  $\mu_t$  n'intervient plus : le prix d'une option d'achat est le même si la tendance de l'actif est haussière ou baissière, ce qui va contre l'intuition première. Cette particularité se retrouvera plus loin avec la valorisation par probabilité neutre au risque.

Lorsque la volatilité  $\sigma(t, x) = \sigma(t)$  ne dépend que du temps de façon déterministe, une solution à l'équation (4) est facilement calculable (faire par exemple un changement de variables  $y = \log(x)$  pour se ramener à l'équation de la chaleur) : cela conduit à la célèbre formule de Black-Scholes utilisée dans toutes les salles de marché du monde, donnant  $V_0 = u(0, S_0)$  pour la valeur de l'option aujourd'hui.

En fait, le problème de la détermination du prix n'est pas complètement résolu (au moins théoriquement), car il n'est pas clair que le prix déterminé est unique. L'hypothèse d'absence d'opportunité d'arbitrage, fondamentale en finance de marché, va permettre de conclure positivement : « dans un marché très liquide sans coût de transaction et de contraintes sur les quantités  $\delta_t$  en actif risqué, il n'est pas possible de gagner de l'argent à coup sûr à partir d'un investissement nul ». Ainsi, dans l'exemple traité, le prix du *Call* est bien  $V_0$  puisque s'il était supérieur (disons  $V'_0 > V_0$ ), il suffirait de vendre un tel contrat et, avec la prime, de suivre la stratégie  $(\delta_t = \partial_x u(t, S_t))_{0 \leq t \leq T}$  pour finalement générer à coup sûr un profit  $V'_0 - V_0 > 0$  à partir de rien. Cette notion d'arbitrage a largement contribué au développement de la finance moderne, en mettant l'accent sur la cohérence des prix de produits dérivés entre eux. Notons enfin que les arguments précédents de valorisation n'utilisent pas de techniques probabilistes, mais seulement un raisonnement trajectorien (à condition de savoir que la variation quadratique de  $(S_t)_{t \geq 0}$  est absolument continue par rapport à la mesure de Lebesgue avec pour densité  $\sigma^2(t, S_t) S_t^2$ ).

Indiquons maintenant les extensions assez immédiates de l'exemple précédent. Les financiers débordant d'imagination, rapidement d'autres options que le *Call* ont vu le jour : souvent, les flux terminaux  $H$  ne dépendent pas uniquement de la valeur en  $T$  de l'actif risqué, mais de toute sa trajectoire. De plus, il est fréquent que plusieurs

### Encadré 2

## FORMULE DE BLACK-SCHOLES

Le prix de l'option d'achat de maturité  $T$  et de prix d'exercice  $K$  est donné par la fonction

$$\left\{ \begin{array}{l} u(t, x) = x \mathcal{N}[d_1(x/[K e^{-\int_t^T r_s ds}]]) \\ \quad - K e^{-\int_t^T r_s ds} \mathcal{N}[d_0(x/[K e^{-\int_t^T r_s ds}]])], \\ d_0(y) = \frac{1}{\sqrt{\int_t^T \sigma^2(s) ds}} \ln[y] - \frac{1}{2} \sqrt{\int_t^T \sigma^2(s) ds}, \\ d_1(y) = d_0(y) + \sqrt{\int_t^T \sigma^2(s) ds}, \end{array} \right.$$

où  $\mathcal{N}$  est la fonction de répartition de la loi normale, centrée-réduite. La stratégie de couverture associée est donnée à

l'instant  $t$  par  $\delta_t = u'_x(t, S_t) = \mathcal{N}[d_1(S_t/[K e^{-\int_t^T r_s ds}]])]$  parts de l'actif risqué.

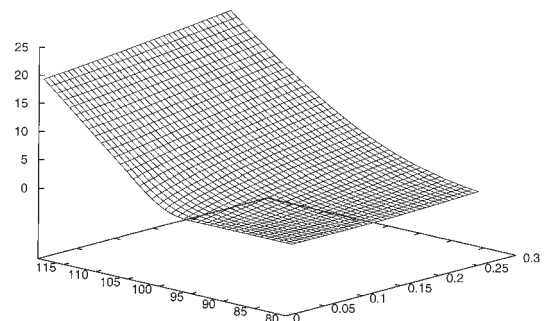


Figure - La surface de prix en fonction de  $x$  et  $T - t$ .

sous-jacents interviennent dans la définition de l'option, et les aléas de ces actifs pourront être modélisés à l'aide de plusieurs mouvements browniens. Si ceux-ci sont en même nombre que les actifs risqués (autrement dit, la matrice de volatilité  $\sigma(t, x)$  est inversible), l'approche précédente pour la valorisation peut être menée à l'identique et il est encore possible de trouver un portefeuille autofinçant atteignant sans risque résiduel le flux promis par l'option : on parle de *marché complet*. Cela conduit dans bien des cas à des équations aux dérivées partielles paraboliques linéaires du second ordre de type (4) avec des conditions frontières à préciser et écrites avec des variables multidimensionnelles : c'est le point d'entrée de l'analyse numérique dans la finance. Ainsi, dans un certain nombre de situations, les méthodes usuelles de résolution numérique pourront être utilisées.

**APPROCHE PLUS PROBABILISTE**

Un autre point de vue que celui du trajectorien et des équations aux dérivées partielles (EDP) est celui basé sur les martingales. Les martingales sont des processus stochastiques dont les accroissements  $M_{t+\delta} - M_t$ , compte tenu de l'information disponible en  $t$ , sont centrés : ces processus ont donc en particulier une espérance (mathématique) constante,  $\mathbf{E}(M_t) = M_0$ . L'équation d'autofinancement (1) se réécrit à l'aide de la valeur actualisée  $\tilde{V}_t = e^{-\int_0^t r_s ds} V_t$

$$d\tilde{V}_t = \delta_t d\tilde{S}_t \tag{5}$$

avec la condition terminale  $\tilde{V}_T = e^{-\int_0^T r_s ds} H := \tilde{H}$ ,  $H$  étant le flux terminal de l'option (par exemple  $H = (S_T - K)_+$ ). Un résultat important relie l'hypothèse d'absence d'opportunité d'arbitrage à l'existence d'une probabilité  $\mathbf{Q}$  sous laquelle l'actif actualisé  $(\tilde{S}_t)_{0 \leq t \leq T}$  est une martingale (voir Föllmer, 2001 et ses références). L'unicité de  $\mathbf{Q}$  est acquise dans les marchés « browniens » décrits précédemment pourvu que la matrice de volatilité  $\sigma(t, x)$  soit inversible. Par l'équation (5),  $(\tilde{V}_t)_{0 \leq t \leq T}$  hérite de la propriété de martingale sous la probabilité  $\mathbf{Q}$  (avec quelques hypothèses sur  $(\delta_t)_{0 \leq t \leq T}$ ) et donc nécessairement

$$V_0 = \mathbf{E}^Q(\tilde{H}) . \tag{6}$$

Ainsi, le prix de l'option est l'espérance des gains actualisés sous une certaine probabilité  $\mathbf{Q}$ . Soulignons que cette dernière n'est qu'un outil de calcul et ne correspond en rien à la probabilité du monde réel. Elle est appelée *probabilité neutre au risque*, car sous celle-ci, la tendance locale de l'actif dans (2) devient  $r_t$  au lieu de  $\mu_t$ .

Le fait que la solution donnée par (4) et (6) coïncide lorsque  $H = (S_T - K)_+$  repose sur le lien classique

entre les EDP (équation de la chaleur et généralisation) et certaines espérances, donné par les formules de Feynman-Kac.

Ramener un prix d'option à un calcul d'espérance a ouvert plusieurs perspectives. Bon nombre de travaux de recherche ont été consacrés (et le sont toujours) aux calculs explicites (en général la plus rapide des approches en terme de temps de calcul), sous-tendant des analyses fines des processus stochastiques et de leur loi (Yor, 2000).

Lorsqu'il n'est pas possible d'obtenir des formules fermées, les méthodes numériques sont à privilégier : hormis les méthodes d'analyse numérique déjà mentionnées, on peut avoir recours aux méthodes de Monte-Carlo, dont le principe est, à l'aide d'un grand nombre  $M$  de simulations indépendantes de scénarios  $\omega_i$ , d'utiliser l'approximation

$$\mathbf{E}^Q(\tilde{H}) \approx \frac{1}{M} \sum_{i=1}^M \tilde{H}(\omega_i) \text{ due à la loi des grands nombres.}$$

La vitesse de convergence est connue pour ne pas être rapide (néanmoins, des techniques d'accélération existent), mais elle est indépendante de la dimension du problème. Ainsi, c'est une alternative intéressante par rapport aux méthodes déterministes, car la dimension des problèmes dépasse souvent 3-4, pour parfois atteindre 40 par exemple (avec les actions de l'indice CAC40). Notons aussi que la simulation de  $\tilde{H}$  passe souvent par celle de fonctionnelle de solutions des équations stochastiques du type (2). Les difficultés proviennent alors de deux sources : d'une part, les fonctionnelles à prendre en compte sont souvent irrégulières (des fonctions des extrêmes de la trajectoire ou même des indicatrices impliquant des temps de sortie...) et, d'autre part, la simulation exacte des équations stochastiques n'est pas simple, notamment lorsque  $\sigma(t, x)$  est non constant. Après avoir stimulé la recherche pendant les 15 dernières années, ces problèmes sont maintenant assez bien maîtrisés (Dupire, 1998). La nécessité de calculer aussi la couverture et plus généralement d'autres sensibilités du prix d'option par rapport à des paramètres a encouragé le développement de méthodes performantes, pour calculer aussi par simulations Monte-Carlo des dérivées d'espérances (Fournié *et al.*, 1999).

**DES PROBLÈMES NON LINÉAIRES**

De nombreux problématiques pertinentes en finance se traduisent en terme d'optimisation non linéaire ou d'EDP non linéaire. Donnons quelques exemples importants.

**Options américaines**

L'option américaine représente le prototype de produits financiers dont il est difficile d'évaluer le prix

numériquement. En effet, cette option confère le droit à son acheteur de choisir l'instant  $\tau \in [0, T]$  où il reçoit son gain  $H_\tau$  (à la différence du cas précédent où nécessairement  $\tau = T$ ). Par les arguments de portefeuille dynamique, le prix de ce produit est égal à  $\sup_{\tau \in [0, T]} \mathbf{E}^Q(e^{-\int_0^\tau r_s ds} H_\tau)$ , le supremum étant pris sur l'ensemble des temps aléatoires  $\tau$  honnêtes (appelés *temps d'arrêt*). Cette quantité peut aussi être vue comme la solution d'une inéquation variationnelle (Bensoussan et Lions, 1978 et Karatzas, 1988). Lorsque la dimension du problème est faible, des méthodes déterministes sont utilisables pour l'évaluation numérique. Dans le cas contraire, on peut utiliser des méthodes de type Monte-Carlo, après avoir d'abord discrétisé les valeurs possibles de  $\tau$  puis utilisé dans ce cadre une équation de programmation dynamique. Même si des progrès importants ont été réalisés depuis cinq ans, les méthodes développées restent coûteuses en mémoire et temps calcul.

### Équations stochastiques rétrogrades et EDP quasi linéaires

L'équation d'autofinancement (5) avec  $\tilde{V}_T = \tilde{H}$  est un cas particulier d'équation du type  $dY_t = f(t, Y_t, Z_t)dt - Z_t dW_t$  avec la condition finale  $Y_T = \xi$  (d'où l'appellation d'équation rétrograde) : la solution est donnée par le couple  $(Y, Z)$ . Comme  $V_t$  était reliée auparavant à une certaine EDP parabolique linéaire du second ordre, il existe aussi des connexions étroites entre les équations rétrogrades et les EDP paraboliques quasi linéaires du type  $\partial_t u = Lu + \tilde{f}(t, x, u, \nabla_x u)$  (avec  $L$  opérateur du second ordre) avec des applications en finance : nous renvoyons à l'article synthétique de Pardoux (1998) et aux références qui y sont données.

### Marché incomplet

Nous avons déjà mentionné que lorsque le nombre de browniens est au plus égal au nombre d'actifs risqués, il existe une gestion de portefeuille parfait, dans le sens que le flux promis  $H$  est atteignable dans tous les scénarios de marché : le risque résiduel  $V_T - H$  est alors nul.

Maintenant, si le nombre de sources d'aléas est supérieur ou si des phénomènes de sauts sur les cours d'actifs sont incorporés dans la modélisation, cette couverture parfaite n'est plus possible en général. Du côté probabiliste, cela correspond à affirmer que l'ensemble  $\mathcal{Q}$  des probabilités neutres au risque est infini. De nombreux critères d'optimisation sont possibles. Une première solution consiste à chercher à dominer avec probabilité 1 le flux terminal :  $V_t \geq H$ . Le plus petit coût à la date d'aujourd'hui de telles stratégies s'appelle le prix de sur-

réplication et est donné essentiellement par  $\sup_{\mathbf{Q} \in \mathcal{Q}} \mathbf{E}^{\mathbf{Q}}(\tilde{H})$  (El Karoui et Quenez, 1995). Malheureusement, cette quantité se révèle être en général très élevée et n'est pas utilisée en pratique. Une alternative consiste à trouver la stratégie de coût  $V_0$  minimal, étant donné un niveau de risque fixé par un critère de type  $\mathbf{E}(l(V_T - H))$  mesurant l'écart entre le flux terminal de l'option  $H$  et la valeur terminale du portefeuille (pour une fonction de perte  $l$ ). À l'aide d'arguments fins de dualité et de techniques de contrôle stochastique (dont l'homologue EDP est l'équation de Hamilton-Jacobi-Bellmann), il est possible de résoudre ces problèmes au moins théoriquement. Pour une synthèse et des références complètes, voir Föllmer (2001).

### ESTIMATION ET CALIBRATION DU MODÈLE

Après s'être concentrés sur la valorisation des contrats financiers le modèle d'actifs étant connu, nous considérons maintenant la question d'identification du modèle : ici, il est primordial de garder à l'esprit sa finalité. Par exemple, les prix d'option d'achat sont nécessairement des fonctions convexes du prix d'exercice  $K$  pour être compatibles avec l'absence d'opportunité d'arbitrage (et ce, quel que soit le modèle) : la détermination d'un modèle (et donc du noyau de valorisation qui en découle) devra respecter cette propriété de convexité.

En dimension 1, une première solution pour l'identification de modèle consiste à supposer une forme *a priori* de type (2) et à chercher à évaluer la fonction de volatilité  $\sigma(t, x)$  (le taux d'intérêt  $r_t$  est moins essentiel car il peut être éliminé par des techniques de changement de numéraire) : ce choix de modèle brownien est assez standard car il est commode à manipuler numériquement. Les données du problème sont des prix d'option d'achat pour quelques échéances et quelques prix d'exercice et par (4). Ces prix d'option sont des solutions d'EDP dont il faut identifier l'opérateur  $L$  : nous sommes en présence d'un problème inverse mal posé. Une difficulté notable réside dans le faible nombre d'observations et les interpolations inévitables ont des conséquences significatives sur le modèle retenu. Des programmes de minimisation des moindres carrés avec pénalisation (Lagnado et Osher, 1995) ou de critère entropique ont été développés.

D'autres approches s'attachent plutôt à estimer le modèle à partir des données d'actifs risqués observées. Ce sont les outils et techniques statistiques qui sont mis en œuvre : nous renvoyons le lecteur à Jarrow (1998) pour un point récent sur ces questions.

En conclusion, ces problèmes sont dans l'ensemble délicats : la pertinence des réponses dépendra des marchés et des produits. Les approches robustes et stables ont évidemment la faveur des praticiens.

**POUR EN SAVOIR PLUS**

**Bachelier (L.)**, « Théorie de la spéculation », *Ann. Sci. école Norm. Sup.*, 1900.

**Bensoussan (A.), Lions (J.-L.)**, « Applications des inéquations variationnelles en contrôle stochastique », *Dunod, Paris*, 1978.

**Black (F.), Scholes (M.)**, « The pricing of options and corporate liabilities », *J. Polit. Econ.*, 81, 637-654, 1973.

**Dupire (B.) (Ed.)**, « Monte Carlo. Methodologies and applications for pricing and risk management », *London : Risk Books*, 1998.

**El Karoui (N.), Quenez (M.-C.)**, « Dynamic programming and pricing of contingent claims in an incomplete market », *SIAM Journal on Control and Optimization*, 33, 29-66, 1995.

**Föllmer (H.)**, « Probabilistic Aspects of Financial Risk », *Proceedings of the European Congress of Mathematics, Barcelona 2000, Birkhäuser*, 2001.

**Fournié (E.), Lasry (J.-M.), Lebuchoux (J.), Lions (P.-L.), Touzi (N.)**, « Applications of Malliavin calculus to Monte Carlo methods in finance », *Finance and Stochastics*, 3, 391-412, 1999.

**Jarrow (R.) (Ed.)**, « Volatility. New estimation techniques for pricing derivatives », *London : Risk Books*, 1998.

**Kahane (J.-P.)**, « Des séries de Taylor au mouvement brownien, avec un aperçu sur le retour », *Development of Mathematics 1900-1950, J.P. Pier (Ed.), Birkhäuser Verlag*, 415-429, 1994.

**Karatzas (I.)**, « On the pricing of American options », *Applied Mathematics and Optimization*, 17, 37-60, 1988.

**Lagnado (R.), Osher (S.)**, « A technique for calibrating derivative security pricing models: numerical solution of an inverse problem », *The Journal of Computational Finance*, 1, 13-25, 1997

**Lamberton (D.), Lapeyre (B.)**, « Introduction au calcul stochastique en Finance », *Collection Mathématiques et Applications 9 – Ellipses*, 1991.

**Merton (R.-C.)**, « Theory of rational option pricing », *Bell J. Econom. and Management Sci.*, 4, 141-183, 1973.

**Pardoux (E.)**, « Backward stochastic differential equations and viscosity solutions of systems of semilinear parabolic and elliptic PDEs of second order », *Stochastic analysis and related topics, VI (Geilo, 1996)*, 42, 79-127, 1998.

**Yor (M.)**, « Le mouvement brownien : quelques développements de 1950 à 1995 », *Development of Mathematics 1950-2000, J.P. Pier (Ed.), Birkhäuser Verlag*, 1187-1202, 2000.

---

**Note de l'auteur**

C'est un plaisir de remercier mes collègues du Centre de mathématiques appliquées pour nos discussions fructueuses.

# Espaces courbes

**La notion d'espace courbe a traversé une très longue maturation. Nous en balisons le cheminement historique en évoquant Newton et la courbure des courbes planes (1665), Gauss et la courbure des surfaces (1827), Riemann et les dimensions supérieures (1854), Einstein et la relativité générale (1916), ou Gromov et les espaces discrets (dès 1980). Le lecteur est également invité à repenser à la différence géométrique entre une feuille de salade et une pelure de pomme, voire à spéculer sur la géométrie de la Toile.**

Le concept d'ESPACE COURBE sert aujourd'hui à modéliser des réalités très diverses. Il apparaît par exemple dans l'étude des défauts cristallins en physique du solide. Il joue également un rôle important dans des appareils de technologie avancée comme le « Global Positioning System » (GPS), qui permettent déjà de localiser un récepteur GPS à quelques mètres près et qui doivent pour cela prendre en compte des effets complexes de relativité générale, eux-mêmes liés à la courbure de l'espace. Certains projets de recherche sont motivés par la prédiction des tremblements de terre : on souhaite un GPS indiquant des déplacements de l'ordre du millimètre (observation des bords des failles de la croûte terrestre dans les zones sismiques), d'où la nécessité de nouvelles études physico-géométriques pour affiner les connaissances et les performances actuelles.

Au cours de l'effort de structuration de nos connaissances, il a fallu un temps considérable pour dégager diverses notions scientifiques fondamentales sous la forme de concepts précis. C'est par exemple le cas de la température en physique, des éléments en chimie, de l'hérédité en biologie... et, précisément, de la courbure en mathématiques. On peut distinguer trois étapes historiques importantes dans l'évolution de ce que l'on entend par « courbure » ; la troisième étape est d'ailleurs en cours.

## RAYON DE COURBURE D'UNE COURBE EN UN POINT

Les courbes présentent certains aspects *globaux* ; par exemple, une courbe peut être dans un domaine limité de l'espace – c'est le cas d'un cercle – ou, au contraire, avoir des points arbitrairement éloignés – c'est le cas d'une droite. Les courbes présentent aussi des aspects *locaux* ; par exemple, un cercle possède une tangente en tout point, alors que le bord d'un carré possède des points (les coins) où la tangente n'est pas définie. Pour les points où la tangente est bien définie, celle-ci est (par définition !) la meilleure approximation locale de la courbe par une droite (figure 1 et détail à la figure 2).

---

– Pierre de la Harpe, Section de mathématiques, Université de Genève, C.P. 240, CH-1211 Genève 24, Suisse.  
pierredelahaarpe@math.unige.ch

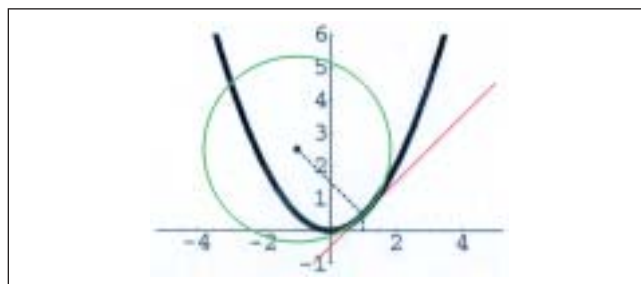


Figure 1

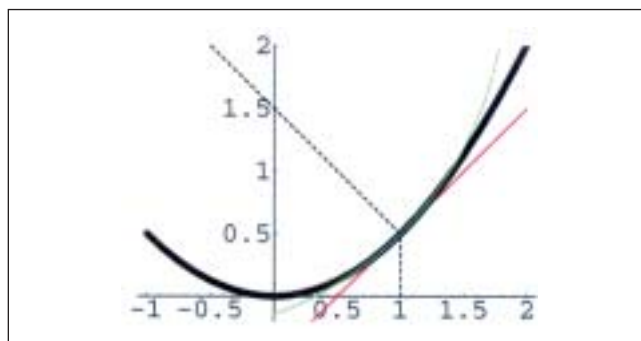


Figure 2

Mais on peut trouver une approximation à la fois meilleure et encore assez simple : le cercle osculateur en un point  $P$  d'une courbe  $C$ , qui est le cercle approchant au mieux  $C$  près de  $P$  (figures 1 et 2). Le rayon de ce cercle est, par définition, le *rayon de courbure* de la courbe  $C$  au point  $P$ .

Ces notions remontent à un travail de 1665 de Isaac Newton (1642-1727) et ont été repensées par de nombreux mathématiciens.

## LE THEOREMA EGREGIUM (THÉORÈME EXCELLENT) DE GAUSS ET LA COURBURE INTRINSÈQUE D'UNE SURFACE

En 1827, Carl Friedrich Gauss (1777-1855) publie un article fondamental qu'il intitule *Disquisitiones generales circa superficies curvas* (Recherche sur la théorie

générale des surfaces courbes)<sup>1</sup>. Gauss a considérablement précisé ce que l'on peut entendre par « surface » et il a su dégager les notions nécessaires pour leur étude. Il a en particulier défini la *courbure totale*  $k(P)$  en un point  $P$  d'une surface  $S$  et a reconnu que c'est un nombre que l'on peut caractériser de plusieurs manières ; en voici une :

$$k(P) = \frac{12}{\pi} \lim_{r \rightarrow 0} \frac{\pi r^2 - \left( \begin{array}{l} \text{aire dans } S \text{ d'un disque} \\ \text{de rayon } r \text{ autour de } P \end{array} \right)}{r^4}$$

(comme l'aire dans un plan d'un disque de rayon  $r$  est précisément  $\pi r^2$ , cette caractérisation montre immédiatement que la courbure d'un plan est nulle en chacun de ses points) ; en voici une autre :

$$k(P) = \frac{3}{\pi} \lim_{r \rightarrow 0} \frac{2\pi r - \left( \begin{array}{l} \text{périmètre dans } S \text{ d'un dis-} \\ \text{que de rayon } r \text{ autour de } P \end{array} \right)}{r^3}$$

(ce qui montre autrement que la courbure du plan est nulle en chacun de ses points).



Figure 3 - Surfaces à courbure nulle : cylindre et cône.

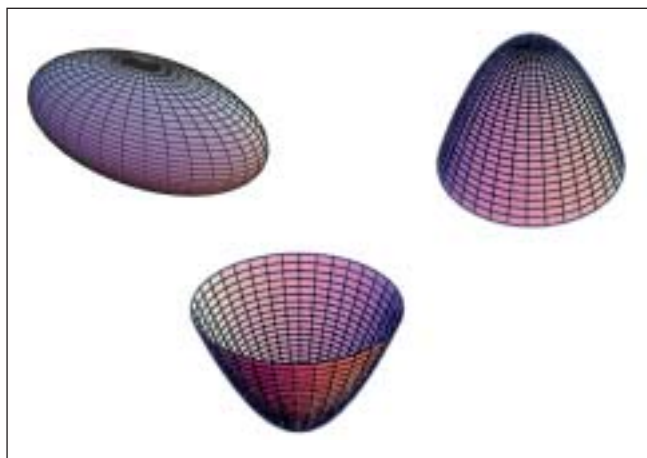


Figure 4 - Surfaces à courbure positive : ellipsoïde, maximum local, minimum local.

<sup>1</sup> Anecdote montrant l'interdépendance des recherches dites pures et appliquées : la période où Gauss trouvait certains de ses résultats fondamentaux sur les surfaces est précisément celle où il travaillait sur mandat gouvernemental à des relevés géodésiques dans le royaume de Hanovre.



Figure 5 - Surfaces à courbure négative : col, hyperboloïde à une nappe.

Il existe de nombreuses manières de mettre en évidence le signe de la courbure. En voici une. Si, dans une surface  $S$ , on découpe une étroite bande circulaire et qu'on l'étale sur une surface plane, on obtient une bande circulaire plane *moins* un secteur lorsque  $S$  est à courbure positive – c'est le cas avec une pelure de pomme. On obtient au contraire une bande circulaire plane dont l'une des extrémités *empiète* sur l'autre lorsque  $S$  est à courbure négative – c'est le cas avec une feuille de salade.

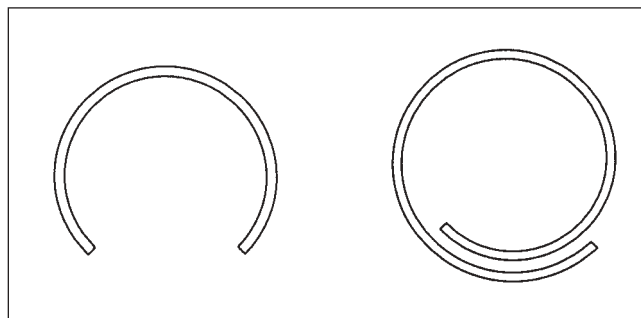


Figure 6 - A propos de pommes et de salade.

Gauss et ses successeurs ont aussi mis en place le concept de *géodésique*, qui précise à la fois :

- (i) la notion de plus court chemin entre deux points d'une surface (en géométrie) ;
- (ii) la notion de trajectoire d'un corps pesant dans un champ de forces extérieures (en mécanique).

On assiste ainsi dans la seconde moitié du XIX<sup>e</sup> siècle à une *géométrisation de la mécanique* qui fut un prérequis important pour les découvertes de la physique quantique et de la relativité au début du XX<sup>e</sup> siècle. Il faut en particulier signaler les visions extraordinaires de Bernhard Riemann (1826-1866). Son œuvre, d'une extrême concision, a changé toutes les mathématiques. Lors de sa leçon d'habilitation (10 juin 1854), il a révolutionné la géométrie, notamment en l'affranchissant du carcan des petites dimensions (1, 2 et 3), et en étendant à son nouveau cadre les notions de distance et de courbure.

Ces travaux ont été menés en même temps que ceux qui ont résolu la controverse millénaire sur « l'axiome des parallèles » d'Euclide (travaux sur la « géométrie

hyperbolique » de Gauss en Allemagne, Lobatchevski en Russie, Bolyai en Allemagne et Hongrie, Beltrami en Italie<sup>2</sup>).

### L'APPROPRIATION DU CONCEPT CHEZ EINSTEIN

Dans la théorie de la relativité, dont les premiers articles ont été publiés en 1905 (relativité restreinte) et 1916 (relativité générale) par Albert Einstein (1879-1955), les lois de la physique s'expriment dans un espace « à 4 dimensions » englobant les trois dimensions usuelles et le temps. En relativité générale, la donnée essentielle de l'espace est sa courbure locale, conformément aux définitions de Gauss et Riemann. Einstein s'est magistralement approprié ces notions puisqu'elles lui permettent d'exprimer la masse des particules : la présence de masse se manifeste ainsi par une simple propriété géométrique de l'espace courbe qui modélise l'espace-temps (Monastyrsky, 1999).

La relativité, née d'un effort de compréhension théorique, a été vérifiée depuis par de nombreuses expériences.

Sur la courbure et la relativité, on trouve quelques idées remarquablement bien exposées dans deux bandes dessinées de Jean-Pierre Petit (1980 et 1981).

### LA NOTION DU SIGNE DE LA COURBURE DANS UN ESPACE DISCRET, LES IDÉES DE GROMOV

Toutes les définitions de courbure évoquées jusqu'ici présupposent une surface ou un espace « continu », et même « lisse » dans un sens à préciser. Mais ce cadre est manifestement trop rigide dans de nombreuses situations : par exemple pour les modèles discrets qu'utilisent de façon constante les ordinateurs (auxquels on ne peut donner qu'un nombre fini d'instructions !). L'extension de la géométrie dans cette direction a été accomplie dans la seconde moitié du xx<sup>e</sup> siècle, en particulier par Alexandrov et Gromov (voir par exemple Gromov, 1994).

Ainsi, étant donné un ensemble fini de points dont on ne connaît que les distances mutuelles, on peut aujourd'hui définir des propriétés de courbure telles que « être à courbure strictement négative » ou « être à courbure positive ». (Exemples de tels ensembles finis de points : les adresses du web [Eckmann et Moses, 2002], ou peut-être les gènes du génome si l'on arrive à définir une notion pertinente de distance entre eux.) Ces notions de courbure permettent des analyses qualitatives tout à fait intéressantes de diverses situations : contenu et transmission de très grandes quantités d'information, ou comportements ergodiques et chaotiques, pour ne citer que deux exemples. Il s'agit là de recherches en cours.

<sup>2</sup> Voilà un bel exemple de la perméabilité des frontières aux idées mathématiques.

L'une des définitions récemment proposées utilise l'idée suivante, qui ne définit pas la courbure proprement dite mais seulement son signe : un espace  $X$  est à courbure strictement négative s'il existe une constante  $D$ , caractéristique de l'espace  $X$ , telle que pour tout triangle dans  $X$  de côtés  $a, b, c$ , tout point de  $a$  est à distance au plus  $D$  d'un point de  $b$  ou de  $c$  ; on dit alors que les triangles sont  $D$ -fins. Dans un tel espace, il peut bien sûr exister des triangles arbitrairement grands (comme en géométrie plane usuelle), mais ces triangles sont néanmoins tous  $D$ -fins pour une même valeur de la constante  $D$  (il n'y a pas d'équivalent des homothéties de la géométrie usuelle).

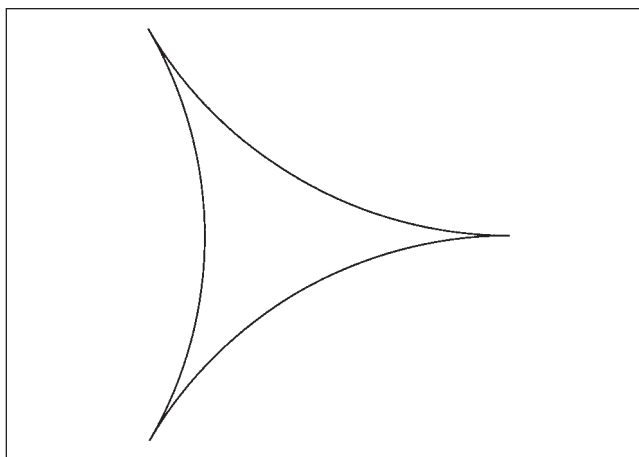


Figure 7 - Un triangle  $D$ -fin.

L'étude géométrique de diverses structures discrètes en mathématique a fait récemment et fait toujours l'objet de travaux de recherche intenses, comme en témoignent parmi beaucoup d'autres les livres de Ghys et de la Harpe (1990), Bridson et Haefliger (1999) et de la Harpe (2000).

### UN RÉSULTAT DE GROMOV EN THÉORIE DES GROUPES

Pour les lecteurs ayant pratiqué davantage de mathématiques, voici quelques éléments permettant d'énoncer au moins un résultat de Gromov, à titre d'échantillon des progrès spectaculaires qu'il a permis en théorie des groupes.

On considère un groupe  $G$  qui est engendré par une famille finie  $\{s_1, s_2, \dots, s_N\}$  d'éléments, au sens où tout élément de  $G$  s'écrit d'une manière au moins comme produit de ces « générateurs »  $s_j$  et de leurs inverses. Pour deux éléments  $g, h$  du groupe  $G$ , on définit la distance  $d(g, h)$  entre  $g$  et  $h$  comme suit : d'abord  $d(g, h) = 0$  si  $g = h$  ; ensuite  $d(g, h) = 1$  si  $g \neq h$  et s'il existe un générateur  $s_j$  tel que  $h = gs_j$  ou  $h = gs_j^{-1}$  ; et dans les autres cas  $d(g, h) = n$  où  $n$  est le plus petit entier tel qu'il existe des éléments  $g = g_0, g_1, \dots, g_n = h$  dans  $G$  avec  $d(g_0, g_1) = d(g_1, g_2) = \dots = d(g_{n-1}, g_n) = 1$ . Pour  $g$  et  $h$  dans  $G$ , une telle suite ( $g = g_0, g_1, \dots, g_n = h$ ) est un segment géodésique

(penser à « segment de droite ») dans le groupe  $G$ . Il est naturel de définir un *triangle* de sommets  $g, h, k$  dans  $G$  comme la réunion de trois segments géodésiques ( $g = g_0, g_1, \dots, g_n = h$ ), ( $h = h_0, h_1, \dots, h_p = k$ ) et ( $k = k_0, k_1, \dots, k_q = g$ ) ; les longueurs des côtés d'un tel triangle sont alors  $n, p$  et  $q$ .

Un groupe  $G$  est dit à *courbure strictement négative*, ou *hyperbolique au sens de Gromov* s'il existe une famille génératrice  $\{s_1, s_2, \dots, s_N\}$  et un nombre réel  $C > 0$  tels que la propriété suivante soit satisfaite : avec les notations ci-dessus, pour tout triangle de  $G$  et pour tout point  $g_i$  sur l'un de ses côtés, il existe un point  $h_j$  ou  $k_l$  sur l'un des *autres* côtés à distance au plus  $C$  de  $g_i$  (comparer avec la figure 7).

Dans un article déjà célèbre de 1987 et dans d'autres plus récents, Gromov a notamment montré des résultats que nous tentons d'évoquer comme suit.

**Théorème.** (i) *Presque tous les groupes qui peuvent être engendrés par une famille finie d'éléments sont à courbure strictement négative.*

(ii) *Pour  $N \geq 2$ , presque tous les groupes à  $N$  générateurs sont de dimension cohomologique 2.*

Un tel énoncé utilise des mots dont il faudrait bien sûr préciser soigneusement le sens. Contentons-nous ici de deux commentaires nécessairement bien vagues. Le premier pour dire que l'on peut considérer simultanément tous les groupes du type indiqué dans le théorème (appelés les *groupes de type fini*) et définir sur cet ensemble une structure convenable pour laquelle les mots « presque tous les groupes » de (i) ont un sens mathématiquement précis. Le second pour dire que, outre la courbure, on sait adapter de nombreux concepts géométriques à des objets « discrets » comme les groupes de type fini ; en particulier, un tel groupe a d'abord une « dimension » (que les professionnels qualifient de cohomologique pour des raisons qui leur sont propres) ; et cette dimension est presque toujours exactement 2, comme celle d'une surface, et non pas 1, comme celle d'une droite, ou 6, comme la dimension de l'espace des positions d'un corps solide dans l'espace.

Avant ces travaux, tous les résultats importants de théorie des groupes concernaient telle ou telle famille particulière de groupes. Gromov a ouvert une vision globale en ce sens qu'elle concerne la *majorité* des groupes, ce qui a très profondément marqué le sujet. (Gromov et bien sûr d'autres, la recherche mathématique est le fait d'une communauté !)

## POUR EN SAVOIR PLUS

**Bourguignon (J.-P.)**, *Espaces courbes*, in « Qu'est-ce que l'univers ? », Université de tous les savoirs, sous la direction d'Y. Michaud, vol. 4, Odile Jacob, 2001, p. 152-163.

**Bridson (M.) et Haefliger (A.)**, *Metric spaces of non-positive curvature*, Die Grundlehren der mathematischen Wissenschaften, Band 319, Springer, 1999.

**Einstein (A.)**, *Die Grundlage der allgemeine Relativitätstheorie*, 1916.

**Eckmann (J.-P.) et Moses (E.)**, *Curvature of co-links uncovers hidden thematic layers in the World Wide Web*, Proc. Natl. Acad. Sci. USA, vol 99:9, 2002, p. 5825-5829 (electronic).

**Gauss (C.-F.)**, *Disquisitiones generales circa superficies curvas*, 1827 ; Werke, IV, 1973, p. 217-258.

**Ghys (E.) et de la Harpe (P.) (éditeurs)**, *Les groupes hyperboliques d'après Mikhael Gromov*, Birkhäuser, 1990.

**Gromov (M.)**, *Hyperbolic groups*, in « Essays in Group Theory », S.M. Gersten, Editor, M.S.R.I. Publ. **8**, Springer, 1987, p. 75-263.

**Gromov (M.)**, *Sign and geometric meaning of curvature*, Rend. Sem. Mat. Fis. Milano, vol 61, 1994, p. 9-123.

**de la Harpe (P.)**, *Topics in geometric group theory*, University of Chicago Press, 2000.

**Monastyrsky (M.)**, *Riemann, topology, and physics*, Birkhäuser, 2<sup>e</sup> édition, 1999.

**Petit (J.-P.)**, *Le géométricon*, Les aventures d'Anselme Lanturlu, Librairie Belin, 1980.

**Petit (J.-P.)**, *Le trou noir*, Les aventures d'Anselme Lanturlu, Librairie Belin, 1981.

**Riemann (B.)**, *Ueber die Hypothesen, welche der Geometrie zu Grunde liegen*, leçon d'habilitation, 10 juin 1854 ; Gesammelte mathematische Werke, 2<sup>e</sup> édition, 1990, p. 304-319.

**Stillwell (J.)**, *Mathematics and its history*, Springer, 1989.

### Note de l'auteur

A de minimes modifications près, ce texte est repris d'un document préparé pour une journée « Portes ouvertes » à l'université de Genève, le 10 mars 2001. C'est un plaisir de remercier Boris Ischi qui a composé les figures.



# Pavages, arbres et labyrinthes aléatoires

**Nous donnons un aperçu de quelques développements récents concernant le comportement à grande échelle de pavages aléatoires ou de labyrinthes aléatoires. On répond ainsi à des questions d'apparence simple : si l'on choisit au hasard (parmi les nombreuses possibilités) un pavage d'un grand domaine par des dominos  $2 \times 1$ , que peut-on dire ? Y a-t-il une limite continue ?**

L'étude à grande échelle de systèmes formés d'une multitude de composantes microscopiques aléatoires constitue l'une des problématiques fondamentales de la physique statistique ainsi que du calcul des probabilités. Souvent, on souhaite évaluer une grandeur macroscopique qui décrit ce système (qui peut être une somme ou une moyenne, comme la magnétisation globale ou la pression). Cela peut être compliqué, en particulier lorsque les composantes interagissent fortement entre elles.

Deux cas peuvent se produire lorsque la taille du système devient grande. Dans le premier, l'observable macroscopique devient déterministe. En d'autres termes, on tend à observer toujours une valeur donnée  $x$  (avec une probabilité grande, on observe une valeur proche de  $x$ ).

L'exemple le plus simple est celui de  $n$  variables aléatoires  $X_1, \dots, X_n$  indépendantes qui prennent chacune les valeurs 1 et  $-1$  avec probabilité  $1/2$  (en d'autres termes, on tire  $n$  fois à pile ou face et  $X_n$  vaut  $-1$  ou  $1$  suivant si le résultat du  $n$ -ième lancer est pile ou face). La moyenne  $(X_1 + \dots + X_n)/n$  des  $n$  valeurs observées (qui est reliée à la proportion du nombre d'observations « face ») est en fait proche de zéro. C'est la loi des grands nombres. Plus généralement, dans des systèmes physiques, les grandeurs thermodynamiques (comme par exemple la pression) peuvent être vues comme une quantité (déterministe) mesurée à partir du mouvement désordonné (aléatoire) d'une multitude de particules (c'est la base de la physique statistique).

Il se peut aussi que la quantité observée à grande échelle soit elle-même aléatoire. On peut malgré tout la décrire par l'intermédiaire de sa distribution. Dans l'exemple ci-dessus, on sait que lorsque  $n$  tend vers l'infini, la loi de  $(X_1 + \dots + X_n)/\sqrt{n}$  tend vers une loi gaussienne. En d'autres termes, pour tout  $a < b$  fixés, la probabilité pour que la quantité aléatoire  $(X_1 + \dots + X_n)/\sqrt{n}$  tombe dans l'intervalle  $(a, b)$  devient de plus en plus proche de

$(2\pi)^{-1/2} \int_a^b e^{-x^2/2} dx$ . C'est le théorème de la limite centrale. On peut le généraliser en disant que la trajectoire d'une marche aléatoire très longue convenablement renormalisée ressemble à une courbe continue aléatoire, le mouvement brownien.

Mis à part le mouvement brownien et les objets (comme les solutions d'équations différentielles stochastiques) qui lui ressemblent, on connaît en fait très peu d'exemples pour lesquels on est capable de décrire mathématiquement un comportement macroscopique aléatoire. En particulier, la modélisation de systèmes où les composantes microscopiques ne sont pas indépendantes (qui constitue la majorité des phénomènes aléatoires autour de nous : on peut par exemple penser à la forme d'un nuage) pose des problèmes.

Récemment, dans un cadre assez particulier, les mathématiciens ont commencé à être capables d'appréhender de tels comportements aléatoires. Il s'agit de l'étude de systèmes aléatoires bidimensionnels dits « critiques » pour lesquels les physiciens théoriciens avaient depuis une vingtaine d'années prédit un comportement macroscopique aléatoire particulièrement intéressant (en particulier leur « invariance conforme »). Il y a eu ces dernières années de nombreux travaux sur ce sujet (l'étude de la percolation critique, les marches aléatoires en dimension 2, etc.) mais nous ne nous focaliserons dans cet article que sur un modèle particulier qui entre dans ce cadre. En fait, ce modèle peut être formalisé de quatre manières équivalentes que nous allons décrire maintenant.

## PAVAGE PAR DOMINOS

Le modèle est élémentaire. On se donne un carré  $N \times N$  où  $N$  est un nombre pair. On dispose d'une boîte contenant  $N^2/2$  dominos de taille  $2 \times 1$ . On choisit alors au hasard (uniformément parmi toutes les solutions possibles, qui sont nombreuses si  $N$  est grand) un recouvre-

**Encadré 1**

**LE MOUVEMENT BROWNIEN PLAN**

Supposons qu'un domaine ouvert plan  $D$  contenant l'origine  $0$  soit donné (par exemple un carré), et considérons une marche aléatoire simple sur la grille carrée de maille  $\delta$ , issue de  $0$  et arrêtée au premier instant  $N$  où elle quitte  $D$ . En d'autres termes, à chaque pas, la marche bouge de  $\delta$  dans l'une des quatre directions cardinales choisie au hasard. Elle part de l'origine et s'arrête lorsqu'elle quitte  $D$ . Lorsque  $\delta \rightarrow 0$ , la loi de la trajectoire de la marche aléatoire converge vers celle d'une trajectoire  $\gamma$  continue aléatoire : celle d'un mouvement brownien plan issu de  $0$  et arrêté au premier instant de sortie de  $D$ . Paul Lévy a observé que si  $\Phi$  est une transformation conforme (i.e. une bijection qui préserve les angles) du domaine  $D$  dans le domaine  $D'$  telle que  $\Phi(0) = 0$ , alors  $\Phi(\gamma)$  est la trajectoire d'un mouvement brownien arrêté lorsqu'il quitte  $D'$  : c'est l'invariance conforme du mouvement brownien plan.

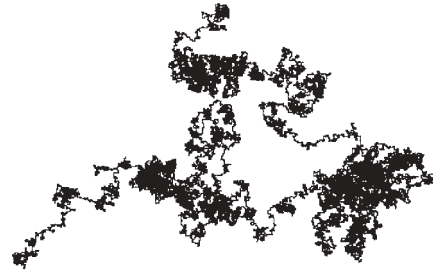


Figure - La trajectoire d'une longue marche aléatoire.

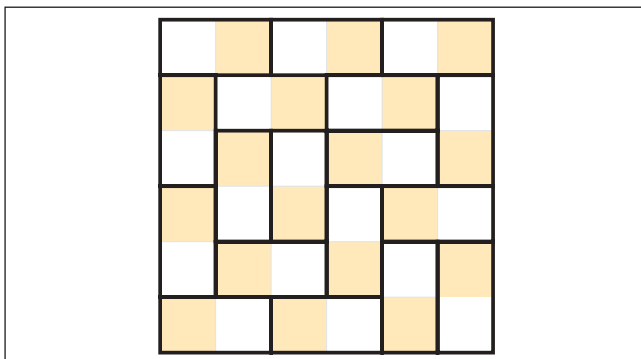


Figure 1 - Un pavage d'un carré  $6 \times 6$ .

ment du carré par ces dominos. C'est un pavage aléatoire. La figure 1 représente un pavage d'un carré de côté 6, où l'on a également colorié le carré à la manière d'un échiquier (cases jaunes et cases blanches).

**ARBRES**

Il existe une bijection naturelle entre l'ensemble des pavages du carré  $N \times N$  et un certain ensemble d'« arbres » que nous allons maintenant décrire. Supposons que l'on indice les petits carrés (de l'échiquier) par leurs coordonnées cartésiennes, de sorte que le petit carré en bas à gauche a pour coordonnées  $(0, 0)$  alors que celui en haut à droite a pour coordonnées  $(N - 1, N - 1)$ . On s'intéresse au graphe plan formé par tous les points à coordonnées paires dans le carré, auquel on rajoute un point « extérieur » au carré qui est relié à tous les points d'abscisse ou d'ordonnée égale à  $N - 1$ . On dit qu'un sous-graphe de ce graphe est un *arbre* s'il n'a qu'une composante connexe, mais pas de cycle. On peut le représenter comme nous l'avons fait à la figure 2 (c'est le

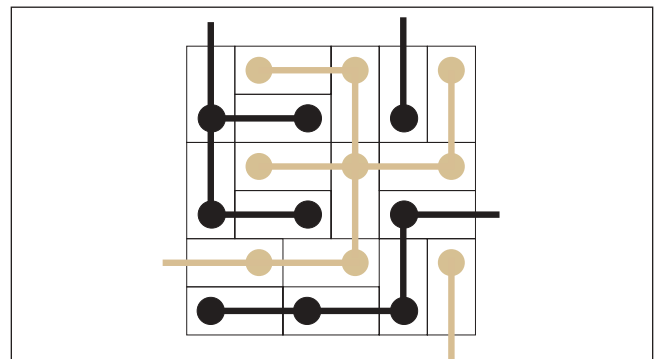


Figure 2 - Le pavage et les arbres associés.

graphe noir) sous la forme d'une famille de petits arbres disjoints attachés aux bords droit et supérieur du carré. Cet ensemble d'arbres est en fait en bijection avec l'ensemble des pavages : si un tel arbre est donné, on dispose des dominos le long des chemins partant des points pairs en direction de l'extérieur. On a ainsi disposé  $N^2/4$  dominos (il y en a un par point pair du carré). Puis on complète le pavage de l'unique façon possible avec les  $N^2/4$  dominos « restants ». En observant la figure, on constate un phénomène de dualité : on aurait pu aussi étudier l'arbre « dual » qui y est dessiné en jaune (qui joint les points à coordonnées impaires aux bords inférieur et gauche). On aurait commencé par disposer les  $N^2/4$  dominos « restants » et complété le pavage avec les dominos qui vont le long de l'arbre noir.

**LABYRINTHES**

Une troisième manière de coder le pavage se fait par l'intermédiaire du labyrinthe qui passe « entre » l'arbre

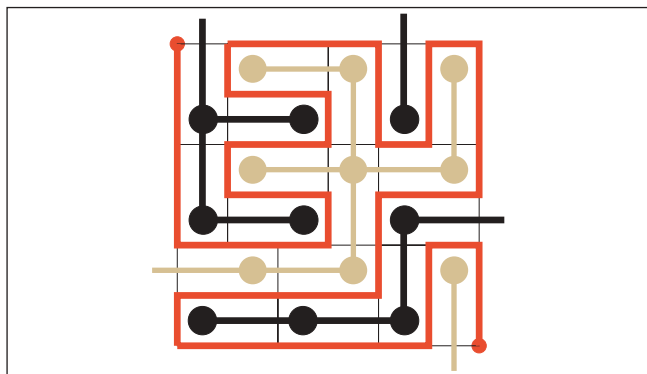


Figure 3 - Le pavage  $6 \times 6$ , les arbres et le labyrinthe associés.

noir et son dual jaune. Plus précisément, on peut tracer le contour de l'arbre noir (qui est aussi le contour de l'arbre jaune) c'est-à-dire l'ensemble des points à égale distance des graphes noirs et jaune. C'est un chemin qui part du coin supérieur gauche du carré pour finir au coin inférieur droit. Notons que ce chemin passe par tous les points constituant les coins des petits carrés de l'échiquier et qu'il n'a pas de point double. Inversement, si un tel chemin est donné, il est facile de lui associer un arbre dont il est le contour : il y a bien une bijection entre l'ensemble de ces chemins couvrants et l'ensemble des arbres (et donc aussi l'ensemble des dominos).

### MARCHES A BOUCLES EFFACÉES

Comment choisir au hasard et uniformément un pavage aléatoire d'un carré ? Le nombre de pavages d'un

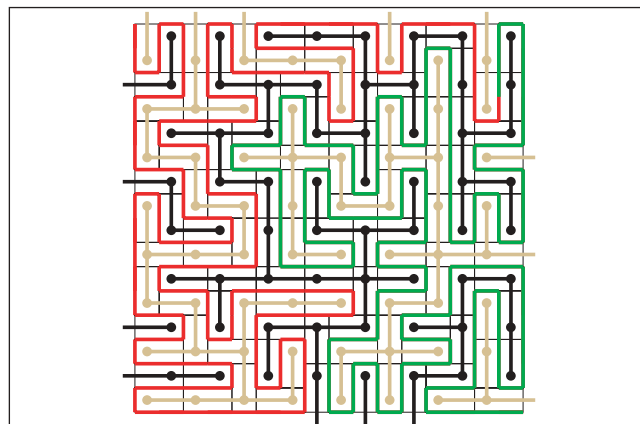


Figure 4 - Un pavage  $16 \times 16$ , l'arbre noir, son dual jaune. Le début du labyrinthe est en rouge, la fin en vert.

carré  $N \times N$  croît exponentiellement avec  $N^2$  de sorte qu'il est difficile d'énumérer tous les pavages et d'en choisir un au hasard. Il existe plusieurs algorithmes beaucoup plus rapides qui permettent de construire un tel pavage aléatoire. Le plus performant est dû à David Wilson et démontre un lien étonnant entre les arbres aléatoires et les marches aléatoires à boucles effacées.

Définissons maintenant ces marches à boucles effacées : supposons qu'un marcheur parte d'un point  $a$  du carré. On se donne aussi un ensemble  $B$  de points du carré. A chaque pas, le marcheur choisit au hasard l'un de ses voisins (s'il est sur le bord du carré, il peut y avoir moins de quatre voisins) et s'y déplace. Lorsqu'il atteint  $B$  (soit  $b$  le point où il atteint  $B$ ), il s'arrête. A partir de la trajec-

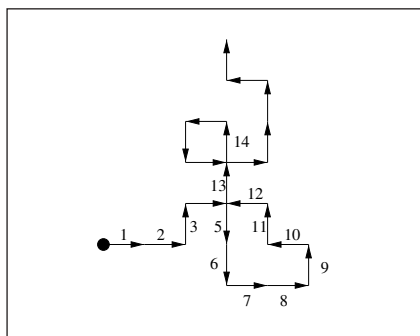


Figure 5 - (a).

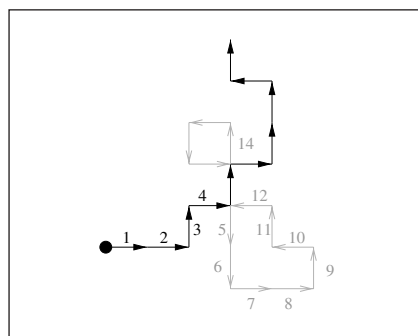


Figure 6 - (b).

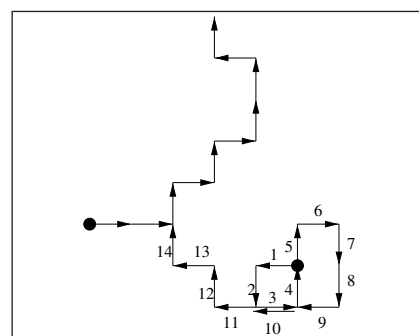


Figure 7 - (c).

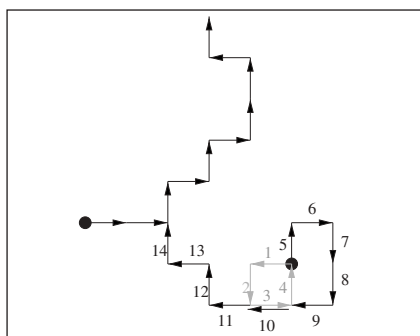


Figure 8 - (d).

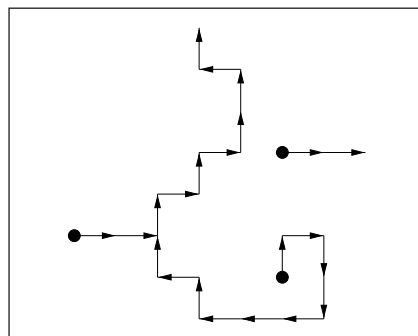


Figure 9 - (e).

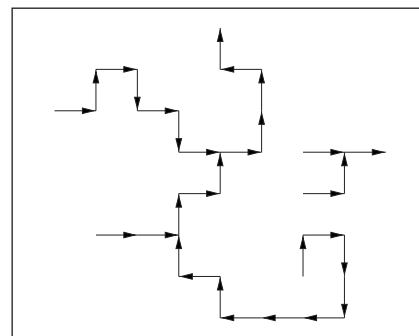


Figure 10 - (f).

toire du marcheur de  $a$  au point  $b \in B$ , on construit une trajectoire *sans points doubles* de la manière suivante : on efface de manière chronologique les boucles effectuées par le marcheur au fur et à mesure qu'elles apparaissent. La courbe aléatoire de  $a$  à  $B$  ainsi obtenue s'appelle la marche aléatoire à boucles effacées de  $a$  à  $B$ .

Décrivons maintenant l'algorithme de Wilson qui montre en particulier que les branches d'un arbre aléatoire uniforme sont en fait distribuées comme des marches à boucles effacées. On construit l'arbre de manière récursive. On se donne un ordre quelconque  $(x_1, \dots, x_n)$  des points dans le carré et on note  $L_0$  la réunion des bords supérieur et droit du carré. On définit alors une marche aléatoire à boucles effacées  $\gamma_1$  (dans le carré) de  $x_1$  à  $L_0$ . On pose  $L_1 = \gamma_1 \cup L_0$ . Puis, on définit une marche aléatoire  $\gamma_2$  à boucles effacées de  $x_2$  à  $L_1$  (si  $x_2$  est déjà sur  $L_1$ , alors  $\gamma_2$  est de longueur nulle). Par récurrence, pour tout  $j$ , on définit une marche aléatoire à boucles effacées  $\gamma_j$  de  $x_j$  à  $L_{j-1}$  et on pose  $L_j = L_{j-1} \cup \gamma_j$ . Par définition,  $L_n$  est un arbre qui passe par tous les points  $x_1, \dots, x_n$ . Wilson a démontré que sa loi est en fait celle d'un arbre aléatoire uniforme. Les figures 5 à 10 illustrent la construction dans le cas du carré lorsque  $L_0$  est la réunion du bord droit et du bord supérieur.

**LE NOMBRE DE POINTS**

On se pose la question suivante : considérons que  $N$  est très grand. Choisissons le point  $A$  au centre du carré (par exemple). Sur l'arbre aléatoire uniforme, il existe un unique chemin (sans point double) reliant  $A$  au bord du carré (c'est-à-dire à la partie  $L_0$  supérieure/droite du bord du carré). L'algorithme de Wilson nous dit que cette courbe est distribuée comme une marche aléatoire à boucles effacées dans le carré de  $A$  à  $L_0$ . On veut connaître l'ordre de grandeur de la longueur de cette courbe. On sait d'après le théorème central limite qu'avant l'effacement des boucles, l'ordre de grandeur du nombre de pas de la marche aléatoire est  $N^2$ . Combien (typiquement) en restera-t-il après ? En exploitant le lien avec les pavages par dominos et par des considérations assez compliquées, il est possible de montrer que la moyenne de la longueur de cette marche à boucles effacées est de l'ordre de  $N^{5/4}$ , ce qui confirme des prédictions effectuées par les physiciens théoriciens (dans ce cas précis, Satya Majumdar ; des exposants étroitement reliés ont été prédits par Bertrand Duplantier).

**STATISTIQUES LOCALES**

Dans une configuration aléatoire de dimères, on peut se poser la question de connaître la probabilité de trouver un certain motif en un point donné. Par exemple, quelle est la probabilité de trouver un domino couvrant à la fois la case  $(x, y)$  et la case  $(x + 1, y)$ ? Cette probabilité vaut

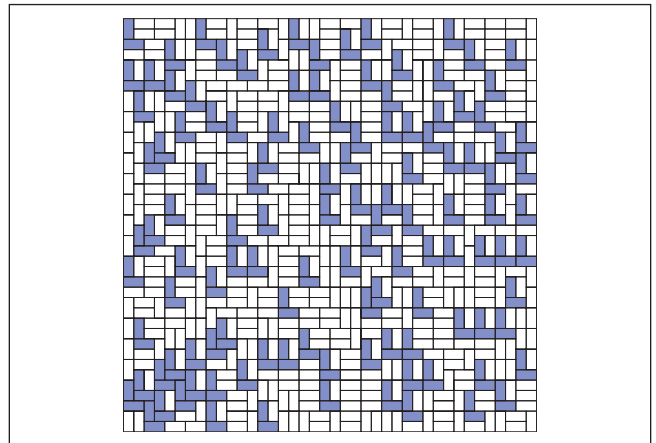


Figure 11 - Un pavage et ses motifs en forme de L.

$1/4$ , car le domino qui couvre la case  $(x, y)$  a des chances égales de couvrir les quatre cases adjacentes. En revanche, la probabilité de trouver un motif composé de plusieurs dominos différents peut avoir une expression plus compliquée. Par exemple, la probabilité de trouver dans une configuration aléatoire un domino couvrant  $(x, y)$  et  $(x + 1, y)$  et en même temps un domino couvrant  $(x, y + 1)$  et  $(x, y + 2)$  (un motif en 'L') vaut  $1/4\pi$ . Dans la figure 11, on voit une configuration aléatoire où les motifs de ce type ont été coloriés. Ces motifs couvrent en moyenne une fraction  $1/\pi$  de l'aire.

**LA LIMITE CONTINUE ?**

Les deux résultats exposés ci-dessus (le nombre de points et les statistiques locales) se démontrent en utilisant comme point de départ le fait qu'il est possible d'exprimer le nombre de pavages d'un domaine *via* des déterminants, dont on peut ensuite évaluer le comportement asymptotique. Ces calculs donnent des informations précises concernant le comportement en moyenne de certaines quantités (le nombre moyen de points sur une marche à boucles effacées, le nombre moyen de configurations d'une forme donnée).

On peut essayer de manière complémentaire de comprendre l'objet aléatoire qui serait la limite d'échelle (donc continue) des labyrinthes aléatoires et des marches à boucles effacées lorsque l'on fait tendre la maille du réseau vers 0.

L'algorithme de Wilson montre que l'étude asymptotique de la loi des pavages aléatoires (ou des labyrinthes/arbres aléatoires) lorsque  $N \rightarrow \infty$  est très étroitement liée à l'étude du comportement des très longues marches à boucles effacées. Il serait naturel de penser que la limite des marches aléatoires à boucles effacées devrait être une courbe brownienne à boucles effacées. Cependant, les trajectoires browniennes ont une géométrie extrêmement compliquée (il y a par exemple des points de multiplicité infinie), de sorte qu'il n'est pas possible de simplement effacer les boucles dans l'ordre

chronologique sur une trajectoire brownienne, puisqu'il n'y a pas de « première » boucle à effacer (sur tout intervalle de temps, le mouvement brownien fait déjà une infinité de boucles). Il ne semble donc pas possible de définir la limite des marches à boucles effacées en partant d'un mouvement brownien plan. Il faut trouver une autre méthode pour décrire cet objet (et montrer la convergence du discret au continu).

### LA LIMITE CONTINUE !

En fait, il est possible de construire et de décrire les objets continus qui sont la limite du labyrinthe uniforme et de la marche aléatoire à boucles effacées lorsque la maille du réseau tend vers 0. Ces objets sont construits en combinant des outils d'analyse complexe (l'équation de Loewner) et des idées probabilistes. Oded Schramm a introduit en 1999 cette classe de processus et il a été prouvé en 2002 qu'ils sont effectivement la limite d'échelle de ces deux modèles. Comme on peut s'y attendre, la limite des marches à boucles effacées est une courbe aléatoire de dimension de Hausdorff  $5/4$  (mais c'est difficile à prouver). Elle s'appelle l'évolution de Schramm-Loewner (SLE) de paramètre 2. On peut l'interpréter comme étant un mouvement brownien à boucles effacées (malgré la difficulté expliquée plus haut) : en effet, en lui rajoutant des « boucles browniennes », on peut reconstruire un mouvement brownien plan.

La courbe de Peano aléatoire converge quant à elle vers le SLE de paramètre 8. Puisqu'il est la limite d'échelle des labyrinthes aléatoires, on peut heuristique-

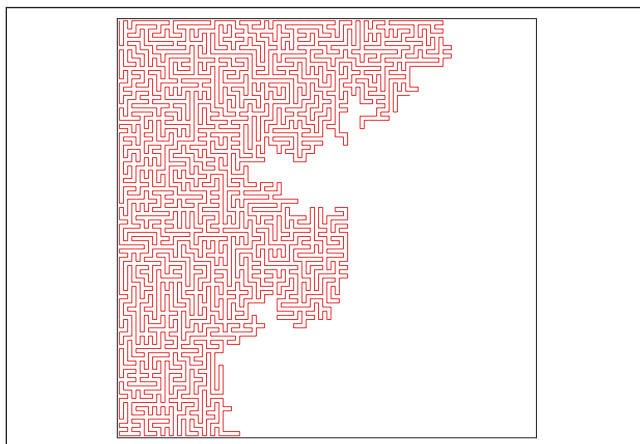


Figure 12 - Le début d'un grand labyrinthe aléatoire.

ment décrire ce processus comme étant une courbe de Peano aléatoire choisie de manière uniforme parmi toutes les courbes de Peano. Il se trouve que cette mesure se concentre en fait sur des courbes particulières : la frontière du domaine recouvert après un certain temps a toujours une dimension de Hausdorff égale à  $5/4$ .

### INVARIANCE CONFORME

Afin de simplifier l'exposé, nous nous sommes focalisés sur le cas du pavage d'un carré. En fait, on aurait pu choisir une forme quelconque, c'est-à-dire un domaine  $D$  simplement connexe (disons borné) du plan. On se donne  $a$  et  $b$  deux points distincts du bord de  $D$  (qui jouent le

### Encadré 2

## LE PROCESSUS DE SCHRAMM

On cherche une courbe aléatoire  $(\gamma_t, t \geq 0)$  infinie issue de 0 dans le demi-plan supérieur  $H$ . A chaque instant  $t$ , on associe à la courbe la transformation conforme  $f_t$  de  $H \setminus \gamma[0, t]$  dans  $H$  telle que  $f_t(\gamma_t) = 0$  et  $f_t(z) \sim z$  lorsque  $z \rightarrow \infty$ . On veut qu'étant donné  $\gamma[0, t]$ , la loi du futur  $f_t(\gamma[t, \infty))$  soit distribuée comme une copie indépendante de  $\gamma$ . En outre, on impose une condition de symétrie : la loi de  $\gamma$  est symétrique par rapport à l'axe imaginaire. Alors, la théorie développée par Charles Loewner dans les années 1920 pour étudier les propriétés des fonctions univalentes, peut être utilisée pour montrer que  $f_t$  (modulo un changement de temps approprié) vérifie l'équation  $df_t(z) = \sqrt{\kappa} dB_t + 2dt/f_t(z)$  où  $B$  est un mouvement brownien unidimensionnel. Cette équation caractérise en fait  $\gamma$  et définit le SLE de paramètre  $\kappa$  qui va de 0 à l'infini dans  $H$ . Par transformation conforme, cela permet de définir les SLE joignant deux points du bord d'un domaine plan simplement connexe (comme par exemple les deux coins opposés d'un carré) : on considère la courbe aléatoire  $\phi(\gamma)$

où  $\phi$  est une transformation conforme de  $H$  dans  $D$  qui envoie 0 et l'infini sur deux points donnés du bord de  $D$ . Il se trouve que le paramètre  $\kappa$  a une grande influence sur les propriétés de la courbe  $\gamma$  ainsi définie. Il a été récemment démontré (mis à part les cas  $\kappa = 2$  et  $\kappa = 8$  détaillés dans cet article) que le SLE de paramètre 6 correspond à la limite d'échelle des interfaces d'un modèle de percolation critique (c'est un travail de Smirnov). La valeur importante  $\kappa = 8/3$  correspond à la frontière extérieure de trajectoires browniennes planes et d'amas de percolation critique, et devrait en outre correspondre à la limite des marches aléatoires auto-évitante (ce serait la loi « uniforme » sur les courbes simples). Il est en fait conjecturé que chaque valeur de  $\kappa$  (au moins dans l'intervalle  $[2, 8]$ ) correspond à la limite d'échelle de modèles discrets issus de la physique statistique. Par exemple  $\kappa = 16/3$  devrait être relié au modèle d'Ising.

rôle des coins du carré précédent). Alors, pour chaque valeur de  $\delta$  (petite), on choisit une approximation adéquate  $D_\delta$  de  $D \cap \delta\mathbb{Z}^2$ , et deux points  $a_\delta$  et  $b_\delta$  approximant  $a$  et  $b$  dans ce graphe. On considère alors un labyrinthe  $\gamma_\delta$  de  $a_\delta$  à  $b_\delta$  (*i.e.* un pavage ou un arbre) aléatoire dans  $D_\delta$ .

Il apparaît (et c'est en fait fondamental pour montrer la convergence dans le cas du carré) que la loi de  $\gamma_\delta$  converge lorsque  $\delta \rightarrow 0$  vers celle d'une courbe de Peano aléatoire (continue) de  $a$  à  $b$  dans  $D$ . Cette courbe a la même loi que l'image de la courbe de Peano aléatoire dans le carré par une application conforme  $\Phi$  du carré dans  $D$  qui envoie les coins (inférieur gauche et supérieur droit) du carré sur  $a$  et  $b$ . L'objet limite est invariant

conforme. C'est ce qui permet de le définir (dans l'encadré 2) d'abord dans le demi-plan supérieur et ensuite dans tout domaine  $D$  en prenant son image par transformation conforme.

Ces problèmes ont aussi un rapport avec d'autres domaines des mathématiques. On peut par exemple montrer que le SLE de paramètre  $\kappa = 2$  est relié à certaines représentations de plus haut poids de l'algèbre de Lie des champs de vecteurs sur le cercle. Comme les physiciens théoriciens l'avaient prédit, ces modèles de prime abord élémentaires sont en fait profonds et relient des domaines mathématiques *a priori* disjoints (analyse complexe, combinatoire, probabilités, représentations).

### POUR EN SAVOIR PLUS

**Kenyon (R.)**, Local statistics of lattice dimers, *Ann. Inst. Henri Poincaré*, 33, 591-618, 1997.

**Kenyon (R.)**, The asymptotic determinant of the discrete Laplacian, *Acta Math.* 185, 239-286, 2000.

**Lawler (G.-F.), Schramm (O.), Werner (W.)**, Conformal invariance of planar loop-erased random walks and uniform spanning trees, *Ann. Prob. (à paraître)*, arXiv:math.PR/0112234, 2001.

**Schramm (O.)**, Scaling limits of loop-erased random walks and uniform spanning trees, *Israel J. Math* 118, 221-288, 2000.

**Wilson (D.-B.)**, Generating random spanning trees more quickly than the cover time, *Proc. 28th ACM*, 296-303, 1996.

# La théorie de Galois et l'arithmétique

**A 20 ans, dans la nuit précédant le duel où il devait trouver la mort, Évariste Galois (1811-1832) écrivit un testament de ses réflexions des années passées. C'était une théorie des équations algébriques que l'on a appelée la théorie de Galois. Aujourd'hui plus que jamais elle est au cœur de l'arithmétique où elle fait se rencontrer l'algèbre, la géométrie, la topologie et l'analyse harmonique.**

Une équation algébrique (à une inconnue  $X$ ) s'écrit  $a_d X^d + a_{d-1} X^{d-1} + \dots + a_1 X + a_0 = 0$ . Quand le degré  $d$  est 1, elle admet la solution  $-a_0/a_1$  dès que les coefficients  $a_0, a_1$  sont éléments d'un ensemble  $F$  où existent les quatre opérations  $+, -, \times$  et  $/$ ; un tel  $F$  est appelé un corps. Quand  $d = 2$ , les solutions sont  $(-a_1 \pm \sqrt{a_1^2 - 4a_0 a_2})/2a_2$ .

De même, pour  $d = 3$  ou  $4$ , les solutions s'expriment en termes des quatre opérations et du passage aux racines  $\sqrt{a}$ ,  $\sqrt[3]{a}$ ,  $\sqrt[4]{a}$  des équations  $X^2 = a$ ,  $X^3 = a$ ,  $X^4 = a$ . Abel a montré que c'est impossible à partir de  $d = 5$ . La théorie de Galois répond à la question la plus générale de savoir déterminer toutes les relations entre équations algébriques à coefficients dans un corps  $F$ . On associe à chacune l'ensemble fini de ses solutions muni de l'action d'un groupe<sup>1</sup>  $G_F$ , le groupe de Galois de  $F$ . Alors les relations entre équations correspondent aux applications entre ensembles finis associés qui respectent l'action de  $G_F$ .

Entre 1958 et 1970, une vision nouvelle et deux généralisations considérables furent apportées à la théorie de Galois par le mathématicien français Alexander Grothendieck, dans le cadre de sa refonte de la géométrie algébrique en « théorie des schémas ». Il définit d'abord les revêtements d'un schéma  $S$  : ce sont les schémas  $S'$  fibrés sur  $S$  et qui localement (au sens de sa « topologie étale ») s'écrivent comme des empilements de copies de  $S$  (tels les étages d'un immeuble au-dessus du sol). Puis il montre que la catégorie<sup>2</sup> des revêtements de  $S$  équivaut à celle des ensembles finis munis de l'action d'un groupe  $\pi_S$ , le « groupe fondamental de  $S$  ». A tout corps  $F$  est

associé un schéma de dimension 0, son « spectre »  $S = \text{Spec } F$ , et les équations algébriques à une inconnue à coefficients dans  $F$  correspondent aux revêtements de  $S$  ; le groupe fondamental  $\pi_S$  n'est autre que le groupe de Galois  $G_F$ . On a donc une généralisation géométrique commune de la théorie de Galois et de celle du groupe fondamental topologique de Henri Poincaré (1854-1912).

Mais de même qu'il y a des schémas de toutes dimensions, il y a au-dessus d'un schéma  $S$  des fibrations de toutes dimensions relatives et non pas seulement de dimension relative 0 comme les revêtements ; quand  $S = \text{Spec } F$ , ce sont les « variétés » définies par des équations algébriques à plusieurs inconnues. Dans cette direction verticale aussi, Grothendieck a donné une généralisation partielle de la théorie de Galois, la « cohomologie  $\ell$ -adique » des fibrations. La cohomologie (ou plutôt l'homologie) d'un espace topologique avait été inventée par Poincaré et, dès les années 1940, André Weil montrait l'intérêt de la transposer en géométrie algébrique. Après des travaux pionniers de Jean-Pierre Serre, Grothendieck a réalisé cette transposition, associant à toute fibration sur un schéma  $S$  des espaces de cohomologie  $\ell$ -adique qui sont des représentations<sup>3</sup> linéaires continues du groupe fondamental  $\pi_S$  ; on parle de représentations galoisiennes de  $S$ . On aurait une généralisation complète de la théorie de Galois si l'on savait remonter de celles-ci aux variétés algébriques ; c'est l'objet de la théorie des « motifs » de Grothendieck qui, aujourd'hui encore, reste conjecturale. En dehors de la dimension relative 0, on ne connaît guère que le cas particulier des variétés dites « abéliennes » qui avait été conjecturé par John Tate et fut démontré par Gerd Faltings en 1983 : quand deux variétés abéliennes ont même cohomologie  $\ell$ -adique, elles se paramètrent l'une par l'autre. Mais s'il est vrai que la catégorie des fibrations (ou plutôt des motifs) sur un schéma de base  $S$  équivaut à celle des représentations galoisiennes de  $S$ , le problème de déterminer ces représentations et leurs relations mutuelles se pose de façon cruciale.

---

– Laurent Lafforgue, Institut des hautes études scientifiques (IHES), Le Bois-Marie, 35 route de Chartres, 91440 Bures-sur-Yvette.  
laurent@ihes.fr

**Encadré 1**

## ÉQUATIONS POLYNOMIALES ET THÉORIE DE GALOIS

L'équation générale du troisième degré, à coefficients complexes par exemple, se résout classiquement en deux étapes. Tout d'abord, on ramène cette équation à la forme

$$P(X) = X^3 - pX + q = 0, \quad p, q \text{ réels}$$

(on élimine le terme en  $X^2$ ),

puis on cherche une racine  $x$  de  $P$  sous la forme :

$$x = u + v \text{ avec la condition } 3uv = p.$$

En développant  $P(u + v)$ , on obtient le système :

$$\begin{cases} u^3 + v^3 = -q \\ u^3 v^3 = \frac{p^3}{27} \end{cases}$$

que l'on sait résoudre :  $u^3$  et  $v^3$  sont les racines du polynôme  $X^2 + qX + \frac{p^3}{27}$ . On aboutit finalement à la « formule de Cardan » :

$$x = \sqrt[3]{\frac{-q}{2} + \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} + \sqrt[3]{\frac{-q}{2} - \sqrt{\frac{q^2}{4} - \frac{p^3}{27}}} \quad (1)$$

donnant bien toutes les racines de  $P$ . En effet, le choix de la première racine cubique impose celui de la seconde, du fait de la relation  $3uv = p$ . L'équation de degré 4 se ramène, par une méthode semblable, à celle de degré 3. La théorie de Galois permet de montrer l'absence d'une formule semblable à (1) pour l'équation de degré 5 ou supérieur, c'est-à-dire de la forme

$P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0 = 0$ , où  $n \geq 5$  et les  $a_i$  sont dans un corps  $\mathbb{K}$ . Pour simplifier, nous supposons ici  $\mathbb{K}$  de caractéristique zéro. L'équation  $P(X) = 0$  est alors dite résoluble par radicaux s'il existe une formule donnant les racines de  $P$  à l'aide d'éléments de  $\mathbb{K}$  et des opérateurs  $+$ ,  $-$ ,  $*$ ,  $/$  et  $\sqrt[n]{\phantom{x}}$ .

Donnons deux définitions essentielles. Un corps de décomposition pour  $P$  est un corps  $\mathbb{L}$  contenant  $\mathbb{K}$ , dans lequel  $P$  a toutes ses racines :

$$P(X) = \prod_{i=1}^n (X - \alpha_i)$$

avec  $\alpha_i \in \mathbb{L}$ , et tel que  $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ . Un tel corps  $\mathbb{L}$  est unique à isomorphisme près. Par exemple, le corps de décomposition de  $X^3 - 2$ , pour  $\mathbb{K} = \mathbb{Q}$ , est  $\mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$ . Le groupe de Galois de cette extension  $\mathbb{L}/\mathbb{K}$ , noté  $\text{Gal}_{\mathbb{L}/\mathbb{K}}$  est le groupe  $\text{Aut}_{\mathbb{K}}\mathbb{L}$  des automorphismes de  $\mathbb{L}$  laissant  $\mathbb{K}$  fixe. Dans l'exemple précédent, ce groupe est le groupe symétrique à trois éléments. Un résultat essentiel dû à Galois affirme que l'équation  $P = 0$  est résoluble par radicaux si et seulement si  $\text{Gal}_{\mathbb{L}/\mathbb{K}}$  est résoluble<sup>1</sup>. En particulier, considérant les coefficients  $a_i$  de  $P$  comme des indéterminées, on peut appliquer ce résultat au corps  $\mathbb{K} = \mathbb{C}(a_0, \dots, a_{n-1})$ .

Le groupe  $\text{Gal}_{\mathbb{L}/\mathbb{K}}$  s'identifie alors au groupe des permutations des racines  $\alpha_i$ . Or ce groupe n'est pas résoluble pour  $n \geq 5$ , d'où l'impossibilité de résoudre par radicaux l'équation générale de degré  $n \geq 5$ , comme l'avait démontré le mathématicien norvégien Niels Henrik Abel (1802-1829).

<sup>1</sup> Un groupe  $G$  est dit résoluble s'il existe des sous-groupes  $G = H_0 \supset H_1 \supset \dots \supset H_n = \{e\}$  tels que  $H_{i+1}$  soit distingué dans  $H_i$  et  $H_i/H_{i+1}$  soit abélien.

L'arithmétique est l'étude des variétés algébriques (et donc des représentations galoisiennes) sur le corps  $\mathbb{Q}$  des fractions. Grothendieck lui associe le point  $\text{Spec } \mathbb{Q}$  mais aussi un schéma de dimension 1,  $\text{Spec } \mathbb{Z}$ , dont les points sont les nombres premiers et sur lequel les fonctions sont les éléments de  $\mathbb{Q}$ . Cela fait ressembler  $\mathbb{Q}$  aux corps de fonctions algébriques sur les courbes. De même qu'une fonction  $f$  sur une courbe a un ordre d'annulation (ou de pôle s'il est négatif)  $v_p(f)$  en tout point  $p$ , de même pour  $f$  une fraction et  $p$  un nombre premier il y a un unique entier  $v_p(f)$  tel que  $f/p^{v_p(f)}$  soit sans facteur  $p$ . Le corps

$\mathbb{Q}$  et les corps de fonctions  $F(C)$  des courbes  $C$  algébriques sur un corps dont le nombre d'éléments est fini sont appelés des corps globaux. A toute représentation galoisienne d'un tel corps on peut associer une fonction analytique  $L$  qui est un produit infini de facteurs indexés par les points de  $\text{Spec } \mathbb{Z}$  ou  $C$ . Ce sont des généralisations de la fonction  $\zeta$  de Riemann  $\left(\zeta(s) = \prod_p \frac{1}{1 - p^{-s}}\right)$  et on s'attend à ce que, comme celle-ci, elles admettent un prolongement analytique et une équation fonctionnelle reliant leurs valeurs en  $s$  et  $1 - s$ . Grothendieck l'a



**Encadré 2**

## VARIÉTÉS ALGÈBRIQUES ET SCHÉMAS

L'objet le plus simple étudié en géométrie algébrique est l'espace affine  $A_{\mathbb{K}}^n$ , où  $\mathbb{K}$  est un corps algébriquement clos. Comme ensemble,  $A_{\mathbb{K}}^n$  est égal à  $\mathbb{K}^n$ . Il est muni d'une topologie, dite de Zariski, dont les fermés sont les ensembles  $V(I)$  de zéros dans  $\mathbb{K}^n$  d'un idéal  $I$  de  $\mathbb{K}[X_1, \dots, X_n]$ . Néanmoins, cette topologie est trop pauvre pour permettre de distinguer suffisamment les variétés algébriques. Il faut donc rajouter de la structure. Pour chaque ouvert  $U \subset A_{\mathbb{K}}^n$ , on définit ainsi les fonctions régulières sur  $U$  comme les applications de  $U$  dans  $\mathbb{K}$  s'écrivant sous la forme  $\frac{P}{Q}$ , où  $P$  et  $Q$  sont deux polynômes,  $Q$  ne s'annulant pas sur  $U$ . Ces fonctions ont une propriété remarquable. En effet, se donner une fonction  $f$  régulière sur  $U$  équivaut à se donner un recouvrement  $\{U_i\}$  de  $U$  par des ouverts, et des fonctions régulières  $f_i$  sur  $U_i$  telles que  $f_i = f_j$  sur  $U_i \cap U_j$ . On dit que la correspondance  $U \mapsto \{ \text{fonctions régulières sur } U \}$  est un faisceau sur  $A_{\mathbb{K}}^n$  (noter l'analogie avec le faisceau des fonctions  $C^\infty$  sur une variété  $C^\infty$ ). Plus généralement, la théorie des schémas de Grothendieck associe à tout anneau commutatif  $A$  un espace topologique, dont les points sont les idéaux premiers de  $A$ , et les fermés les ensembles  $V(I)$  d'idéaux premiers contenant un idéal  $I \subset A$ . Cet espace est muni d'un faisceau d'anneaux, moralement construit de sorte que  $A$  s'identifie aux fonctions régulières sur cet espace. L'objet ainsi créé s'appelle spectre de  $A$ , noté  $\text{Spec}(A)$ . C'est un schéma affine. Les schémas généraux s'obtiennent par recollement de tels schémas. Regardons de plus près  $\text{Spec}(\mathbb{Z})$  et  $\text{Spec}(\mathbb{K}[X])$ . On peut les dessiner ainsi :

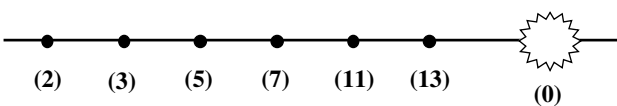


Figure 1 -  $\text{Spec}(\mathbb{Z})$ .

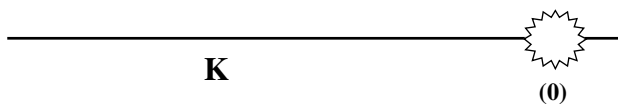


Figure 2 -  $\text{Spec}(\mathbb{K}[X])$ .

Dans les deux cas, l'espace topologique considéré ressemble à une droite avec la topologie des parties finies, plus un point dense  $\eta$  correspondant à l'idéal nul. Si  $\mathbb{K}$  est dénombrable, ces deux espaces sont homéomorphes. Néanmoins, les deux schémas considérés ne sont pas isomorphes : leurs faisceaux de fonctions régulières sont tout à fait différents. Considérons le schéma  $S = \text{Spec}(\mathbb{K}[X_1, \dots, X_n]/(P))$ , où  $P$  est un polynôme irréductible. Les points fermés de  $S$  correspondent aux idéaux maximaux de  $\mathbb{K}[X_1, \dots, X_n]$  contenant  $P$  qui, d'après le théorème des zéros de Hilbert, sont en bijection avec les solutions dans  $\mathbb{K}^n$  de l'équation  $P = 0$  : il en résulte que  $S$  est une hypersurface algébrique.

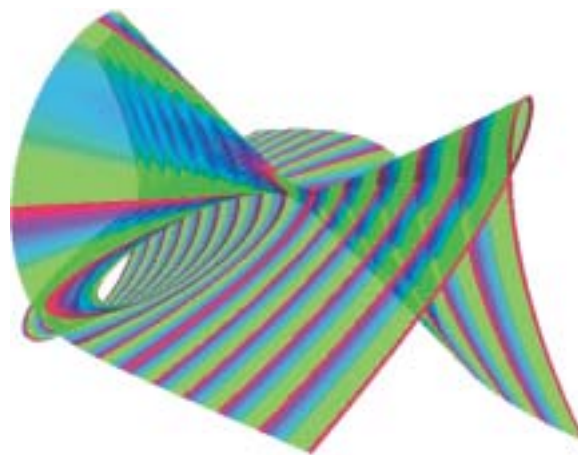


Figure 3 - Une hypersurface algébrique.

Cet exemple, joint à celui de  $\text{Spec}(\mathbb{Z}[i])$  étudié dans l'encadré 3, montre comment la théorie des schémas est une généralisation commune de l'arithmétique et de la géométrie algébrique.

prouvé dans le cas des corps de fonctions comme conséquence d'un résultat venu de la topologie, la « dualité de Poincaré ». Mais on ne connaît toujours pas la dualité sur  $\text{Spec } \mathbb{Z} \dots$

C'est via les fonctions  $L$  que, selon la prédiction du mathématicien canadien Robert Langlands, la théorie de Galois rejoint l'analyse harmonique. Il s'agit de la branche des mathématiques créée au XIX<sup>e</sup> siècle par

Encadré 3

## REVÊTEMENTS ÉTALES ET GROUPE FONDAMENTAL

Nous expliquons ici comment la notion de revêtement, bien connue pour les bons espaces topologiques, se généralise aux schémas. Pour simplifier, tous les schémas seront ici supposés connexes. Nous devons donc traduire en géométrie algébrique la notion d'isomorphisme local qui, transposée naïvement, ne donnerait rien. Un morphisme surjectif entre schémas, qui est un isomorphisme local, est en effet un isomorphisme, car les ouverts de Zariski sont denses pour une classe très large de schémas. Il faut donc raffiner cette topologie, pour en obtenir une nouvelle appelée topologie étale. Ce n'est pas une topologie au sens usuel : elle consiste en la donnée, pour tout schéma  $X$ , de familles de morphismes entre schémas

$\{U_i \xrightarrow{f_i} X\}$  vérifiant certaines propriétés qui axiomatisent la notion de « recouvrement de  $X$  par des ouverts  $U_i \hookrightarrow X$  ».

Les applications  $\{U_i \xrightarrow{f_i} X\}$  considérées ici sont les morphismes étales. Une bonne définition de ces morphismes

est celle du critère jacobien :  $\{U \xrightarrow{f} X\}$  est dit étale si localement  $f$  présente  $U$  à l'aide d'équations polynomiales

$$P_1(X_1, \dots, X_n) = \dots = P_n(X_1, \dots, X_n) = 0 \text{ avec } \det \begin{pmatrix} \delta P_i \\ \delta P_j \end{pmatrix}$$

inversible. On pourrait penser que  $U$  est une bande horizontale étalée sans rebroussement sur  $X$  :

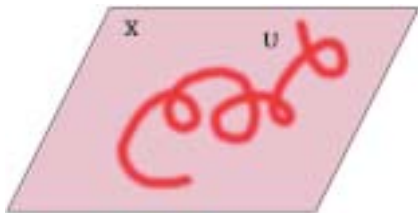


Figure 1

Cela ne reflète cependant pas la richesse de cette notion. Par exemple, si  $X = \text{Spec}(\mathbb{K})$ , alors  $U$  sera du type  $\text{Spec}(\mathbb{L})$ , où  $\mathbb{L}$  est un corps, extension finie séparable de  $\mathbb{K}$ .

Un revêtement entre schémas est, à peu de choses près, un morphisme  $U \rightarrow X$  étale et surjectif. Par exemple,

$\mathbb{C}^* \rightarrow \mathbb{C}^*, x \mapsto x^n$ , est un revêtement étale du schéma

$$\mathbb{C}^* = \text{Spec}(\mathbb{C}[X, \frac{1}{X}]).$$

Comme en topologie, on a la notion de revêtement galoisien, et tout revêtement est en dessous d'un revêtement galoisien. De plus, si  $X = \text{Spec}(\mathbb{K})$ , les revêtements galoisiens correspondent aux extensions de corps galoisiennes.

Bien qu'il n'existe pas en général de revêtement universel pour un schéma  $S$  donné, il existe un groupe fondamental  $\Pi_S$ , dont les quotients finis sont les groupes d'automorphismes des revêtements galoisiens. Il est remarquable, et non trivial, que  $\Pi_{\text{Spec}(\mathbb{Z})} = \{e\}$ , c'est-à-dire que tout corps de nombres

$\mathbb{K}$  est ramifié en au moins un nombre premier  $p$ . Par exemple, le morphisme canonique  $\text{Spec}(\mathbb{Z}[i]) \mapsto \text{Spec}(\mathbb{Z})$  est ramifié au point  $(1+i)$  : si l'on enlève ce point, le morphisme obtenu sera étale. Le morphisme en question peut se dessiner ainsi :

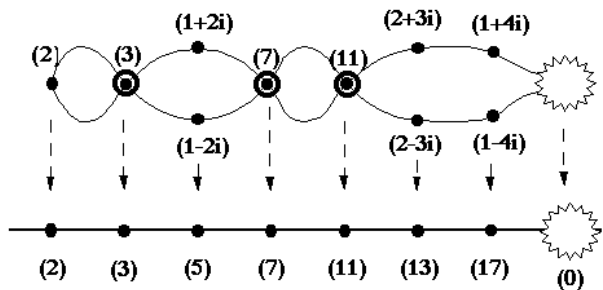


Figure 2

Joseph Fourier pour analyser les ondes et qui étudie les fonctions périodiques, par exemple  $\cos$  et  $\sin$  sur  $\mathbb{R}$  avec le groupe de périodes  $2\pi\mathbb{Z}$ . On associe à un corps global  $F = \mathbb{Q}$  ou  $F(\mathbb{C})$  son « anneau<sup>4</sup> des adèles »  $\mathbb{A}_F$  qui est un produit infini de corps  $F_p$  « localisés de  $F$  » en tous les points  $p$  de  $\text{Spec } \mathbb{Z}$  ou  $\mathbb{C}$ . On appelle automorphes les fonctions sur le groupe  $\text{GL}_r(\mathbb{A}_F)$  des matrices  $r \times r$  inversibles à coefficients dans  $\mathbb{A}_F$  qui admettent  $\text{GL}_r(F)$  comme groupe de périodes ; sous une forme différente leur première étude remonte à Poincaré. A toute représentation automorphe de  $\text{GL}_r(\mathbb{A}_F)$ , Langlands a associé une fonction analytique  $L$ , définie aussi par un produit infini de facteurs indexés par  $p$  et qui admet un prolongement analytique et une équation fonctionnelle. Il

conjectura le fabuleux énoncé suivant : pour tout  $r \geq 1$ , il existe une unique correspondance préservant les fonctions  $L$ ,  $\sigma \mapsto \pi_\sigma$ ,  $\pi \mapsto \sigma_\pi$  entre l'ensemble des représentations galoisiennes  $\sigma$  de dimension  $r$  de  $F$  et celui des représentations automorphes  $\pi$  de  $\text{GL}_r(\mathbb{A}_F)$ .

Le cas  $r = 1$  est une reformulation, déjà connue d'Emil Artin (1898-1962), de la théorie du « corps de classes » qui a occupé tous les arithméticiens au XIX<sup>e</sup> siècle et jusque dans les années 1930. Les cas  $r \geq 2$  sont encore plus subtils car les groupes  $\text{GL}_r(\mathbb{A}_F)$  ne sont plus commutatifs.

Pour  $F = F(\mathbb{C})$  et grâce aux équations fonctionnelles de Grothendieck, on a pu montrer que s'il y a des appli-

**Encadré 4**

## THÉORIE DU CORPS DE CLASSES

Un problème majeur des mathématiques actuelles est la description du groupe de Galois de  $\overline{\mathbb{Q}}/\mathbb{Q}$ . Cette question est extrêmement délicate. Néanmoins, la théorie du corps de classes apporte une réponse partielle. Elle comporte deux volets.

Le premier est local : on s'intéresse aux corps locaux, par exemple les nombres  $p$ -adiques ou les séries formelles sur un corps fini. Le résultat principal est le suivant.

La correspondance :

$$\begin{aligned} & \{\text{extensions finies abéliennes de } \mathbb{K}\} \\ & \longrightarrow \{\text{sous-groupes de } \mathbb{K}^* \text{ d'indice fini}\} \end{aligned}$$

$$\mathbb{L} \longmapsto N_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^*)$$

est bijective,  $N_{\mathbb{L}/\mathbb{K}}$  désignant la norme de l'extension  $\mathbb{L}/\mathbb{K}$ . De plus, on dispose d'un isomorphisme, défini pour toute extension galoisienne  $\mathbb{L}/\mathbb{K}$  :

$$(\alpha, \mathbb{L}/\mathbb{K}) : \mathbb{K}^*/N_{\mathbb{L}/\mathbb{K}}(\mathbb{L}^*) \xrightarrow{\sim} \text{Gal}_{\mathbb{L}/\mathbb{K}}^{ab}$$

jouissant de nombreuses propriétés fonctorielles. On a ainsi une description de  $\text{Gal}_{\mathbb{L}/\mathbb{K}}^{ab}$ , le plus grand quotient abélien de

$\text{Gal}_{\mathbb{L}/\mathbb{K}}$ . Ces résultats peuvent s'obtenir de multiples manières, notamment grâce à la dualité de Nakayama-Tate

entre certains groupes de cohomologie galoisienne.

L'autre volet de la théorie du corps de classes traite des corps globaux. Pour fixer les idées,  $\mathbb{K}$  désigne maintenant un corps de nombres. Le rôle joué dans le cas local par  $\mathbb{K}^*$  est ici tenu par le groupe  $C_{\mathbb{K}} = I_{\mathbb{K}}/\mathbb{K}^*$  des classes d'idèles de  $\mathbb{K}$ . On note ici  $I_{\mathbb{K}}$  le groupe des idèles de  $\mathbb{K}$ , défini pour  $\mathbb{K} = \mathbb{Q}$  par  $I_{\mathbb{Q}} = \mathbb{R}^* \times \prod'_{p \in \mathcal{P}} \mathbb{Q}_p^*$ , où  $\mathcal{P}$  désigne l'ensemble des nombres premiers,  $\mathbb{Q}_p$  le corps des nombres  $p$ -adiques et  $\prod'$  la partie du produit formée des éléments qui sont presque partout des unités. En général, les facteurs du produit définissant  $I_{\mathbb{K}}$  sont les complétés de  $\mathbb{K}$  pour toutes les valeurs absolues de  $\mathbb{K}$ . Ces corps sont  $\mathbb{R}$  ou  $\mathbb{C}$  pour des valeurs absolues archimédiennes et des extensions finies de corps  $p$ -adiques pour les autres. On a alors deux théorèmes analogues aux précédents, en remplaçant  $\mathbb{K}^*$  (resp.  $\mathbb{L}^*$ ) par  $C_{\mathbb{K}}$  (resp.  $C_{\mathbb{L}}$ ). Les ingrédients de la démonstration sont toujours de nature cohomologique, mais également analytique : le théorème de Cebotarev – vaste généralisation du théorème de la progression arithmétique de Dirichlet – intervient à un point crucial de la preuve. En fait, la théorie du corps de classes donne même une description de l'abélianisé de  $\text{Gal}(\overline{\mathbb{K}}/\mathbb{K})$  tout entier pour un corps global  $\mathbb{K}$ . Cela revient à décrire toutes les représentations continues de dimension 1 de  $\text{Gal}(\overline{\mathbb{K}}/\mathbb{K})$  ; c'est en cela que cette théorie coïncide avec le programme de Langlands pour  $r = 1$ .

**Encadré 5**

## REPRÉSENTATIONS AUTOMORPHES

Nous précisons ici la notion de représentation automorphe du groupe  $\text{GL}_r(\mathbb{A})$ . Pour simplifier l'exposé, nous considérons ici un corps  $F$  de fonctions sur une courbe algébrique  $C$  définie sur un corps fini, par exemple  $F = \mathbb{F}_p(t)$ . L'anneau des adèles de  $F$  est ici  $\mathbb{A} = \prod'_{x \in C} F_x$ , où  $F_x$  désigne le corps local obtenu par complétion de  $F$  au point  $x \in C$ , et  $\prod'$  la sous-partie du produit formée des éléments qui sont presque partout des entiers, c'est-à-dire éléments de l'anneau des entiers  $O_x \subset F_x$ .

L'anneau  $\mathbb{A}$  est muni d'une topologie dont une base de voisinages ouverts de 0 est donnée par les ensembles  $\prod_{x \in S} H_x \times \prod_{x \notin S} O_x$ , où  $S \subset C$  est fini et  $H_x \subset F_x$  est ouvert pour  $x \in S$ . On a une injection naturelle  $F \hookrightarrow \mathbb{A}$ .

On appelle forme automorphe sur  $\text{GL}_r(\mathbb{A})$  une fonction  $f : \text{GL}_r(\mathbb{A}) \rightarrow \mathbb{C}$  possédant les propriétés :

- $f$  est invariante à gauche par  $\text{GL}_r(\mathbb{F})$  :  $f(\gamma x) = f(x)$  ( $\gamma \in \text{GL}_r(\mathbb{F})$ ,  $x \in \text{GL}_r(\mathbb{A})$ )

- $f$  est invariante à droite par un sous-groupe ouvert  $H \subset \text{GL}_r(\mathbb{A})$  :  $f(x) = f(xh)$  ( $h \in H$ ,  $x \in \text{GL}_r(\mathbb{A})$ )

En toute rigueur, il faudrait demander une troisième condition que nous omettons ici.

Le groupe  $\text{GL}_r(\mathbb{A})$  opère sur l'espace  $\mathcal{A}$  des formes automorphes par :

$$(g.f)(x) = f(xg) \text{ (avec } f \in \mathcal{A} \text{ et } x, g \in \text{GL}_r(\mathbb{A}))$$

Une représentation automorphe est une représentation irréductible de  $\text{GL}_r(\mathbb{A})$  qui se réalise dans l'espace  $\mathcal{A}$ . Rappelons qu'une représentation  $\rho : G \rightarrow \text{GL}(V)$  est dite irréductible si les seuls sous-espaces de  $V$  stables par  $\rho$  sont  $\{0\}$  et  $V$ . Une représentation automorphe s'écrit toujours comme produit tensoriel infini de facteurs locaux, qui sont des représentations irréductibles des groupes  $\text{GL}_r(F_x)$ .

En cela réside l'aspect local de cette théorie. L'aspect global est quant à lui contenu dans l'invariance à gauche des formes automorphes par le sous-groupe  $\text{GL}_r(F)$ .

cations  $\pi \mapsto \sigma_\pi$  en rangs  $< r$ , il y en a en sens inverse  $\sigma \mapsto \pi_\sigma$  en rangs  $\leq r$ . Pour  $F = \mathbb{Q}$  et en dehors de  $r = 1$ , le cas le plus important de construction  $\sigma \mapsto \pi_\sigma$  connu à ce jour est dû à Andrew Wiles : c'est quand  $\sigma$  provient d'une courbe elliptique (une variété abélienne de dimension 1). D'après le théorème de Faltings cité plus haut, cela signifie que toute courbe elliptique sur  $\mathbb{Q}$  se paramètre par ce que l'on appelle une courbe modulaire et, comme chacun sait, cela implique le théorème de Fermat.

Dans l'autre sens  $\pi \mapsto \sigma_\pi$ , on cherche à trouver les  $\sigma_\pi$  dans la cohomologie  $\ell$ -adique de variétés algébriques sur  $F$  convenables. Pour  $F = F(C)$ , le mathématicien ukrainien Vladimir Drinfeld a proposé au début des années 70 une réponse conjecturale à cette question, les variétés de « chtoucas » ; il démontra le cas  $r = 2$ . Récemment, l'auteur de cet article a généralisé en rang arbitraire la preuve de Drinfeld si bien qu'aujourd'hui la correspondance de Langlands sur les corps de fonctions est démontrée. Sur  $F = \mathbb{Q}$ , une réponse partielle est fournie conjecturalement par des variétés introduites dès avant que Langlands formule son programme par le mathématicien japonais Shimura et qui généralisent les courbes modulaires. Mais la cohomologie de ces variétés ne peut contenir qu'une partie des représentations galoisiennes et, en général, on ne sait pas encore la calculer.

Les théories de Galois et de Grothendieck et le programme de Langlands qui les complète sont une grande

et belle réalisation de l'esprit humain. Nul doute que les problèmes non résolus qu'ils proposent – les motifs, la cohomologie des variétés de Shimura ou d'autres plus générales qui restent à définir, les propriétés des fonctions L des représentations galoisiennes – resteront longtemps à l'horizon de la géométrie algébrique et de l'arithmétique.

### Quelques définitions

(1) Un groupe est un ensemble muni d'une loi de composition  $(g_1, g_2) \mapsto g_1 g_2$ , d'un élément 1 et d'un passage à l'inverse  $g \mapsto g^{-1}$ . Il est dit commutatif ou abélien si l'on a toujours  $g_1 g_2 = g_2 g_1$ .

Une action d'un groupe sur un ensemble fini consiste à associer à tout élément du groupe une permutation des éléments de l'ensemble, de façon compatible avec les lois de composition.

(2) Une catégorie est une collection d'objets et de relations entre ces objets.

(3) Une représentation linéaire d'un groupe est un espace vectoriel muni de transformations linéaires indexées par les éléments du groupe, de façon compatible avec les lois de composition.

(4) Un anneau est un ensemble où existent les trois opérations  $+$ ,  $-$  et  $\times$  mais pas nécessairement la division  $/$ .

# Méthodes mathématiques et analyse numérique pour la chimie moléculaire

**La simulation numérique dans le domaine de la chimie moléculaire et dans les domaines connexes de la biologie moléculaire et de la science des matériaux, est un champ du calcul scientifique en pleine expansion. Les besoins sont énormes. Le tout début de l'histoire est en train de s'écrire. Seule une alliance de méthodes d'analyse mathématique pointues, de techniques d'algorithmique numérique adaptées et avancées et de moyens de calcul d'énorme puissance, permettra d'avoir un impact réel sur l'avancée de la science en ces domaines.**

La chimie théorique, et plus précisément la chimie quantique, a pour but la modélisation des systèmes de taille moléculaire. L'objectif est de comprendre et prévoir les propriétés de la matière à l'échelle macroscopique à partir de la simulation du comportement de ses constituants à l'échelle microscopique. A cette échelle, les briques constitutives de la matière sont les électrons et les noyaux. L'échelle d'espace est l'angström ( $10^{-10}$  m), l'échelle de temps est la femtoseconde ( $10^{-15}$  s). Pour une grande gamme d'applications liées à la chimie, les noyaux peuvent être considérés comme des particules classiques alors que la nature quantique des électrons est essentielle pour la compréhension, notamment, de la réactivité chimique. En considérant la position des noyaux comme connue (elle peut être déterminée expérimentalement, ou numériquement par une boucle d'optimisation externe), l'état d'équilibre d'un système moléculaire constitué d'un assemblage de noyaux et d'électrons est déterminé par la résolution de l'équation de Schrödinger stationnaire pour la fonction d'onde électronique. Parallèlement, son évolution est dictée par la version dépendante du temps de cette équation. Nous nous focalisons ici sur la détermination de l'état stationnaire et n'aborderons les questions d'évolution que dans l'encadré 1.

La détermination de la structure électronique d'équilibre est un véritable défi pour la simulation numérique, la dimension de l'espace de configuration d'un système moléculaire, même de taille réduite et comportant par exemple une dizaine d'atomes, pouvant très vite atteindre plusieurs centaines. Pourtant, cette simulation numérique est aujourd'hui essentielle pour compléter l'observation

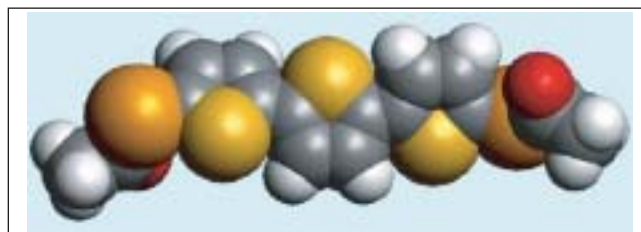


Figure 1 - Un système moléculaire.

expérimentale, car elle en fournit des moyens d'interprétation. Elle peut aussi remplacer cette observation expérimentale, quand cette dernière est impossible. Un exemple typique est l'étude des propriétés de la matière présente au centre de la terre : réaliser des pressions comparables en laboratoire est extrêmement difficile, alors que réaliser la simulation numérique est abordable. Comme le lecteur peut s'en douter au vu du nombre de degrés de liberté en jeu, et comme nous allons le voir, abordable ne veut pas pour autant dire facile.

## UNE HIÉRARCHIE DE MODÈLES

Le problème central de la modélisation en chimie quantique moléculaire, et donc le cœur d'un code de simulation numérique en ce domaine, est la détermination de l'état fondamental électronique du système par la résolution de l'équation de Schrödinger stationnaire

$$H_N \Psi = \varepsilon \Psi \quad (1)$$

ou alternativement du problème de minimisation

---

– Claude Le Bris, CERMICS, École nationale des ponts et chaussées, 6 & 8 avenue Blaise Pascal, 77455 Marne-La-Vallée cedex 2  
tél. : 01 64 15 35 73, lebris@cermics.enpc.fr

Je remercie Éric Cancès, Isabelle Catto, Mireille Defranceschi, Maria Esteban, Pierre-Louis Lions, Yvon Maday, Éric Séré et Gabriel Turinici pour plusieurs années de collaboration et d'interaction fructueuses sur le sujet.

## Encadré 1

**CONTRÔLE DES RÉACTIONS CHIMIQUES**

La possibilité de simuler numériquement de manière efficace une évolution d'un système quantique par l'équation de Schrödinger sous sa forme dépendante du temps

$$i\hbar \frac{\partial \Psi(t, x)}{\partial t} = H(t) \Psi(t, x)$$

(où  $\Psi(t, \cdot)$  désigne la fonction d'onde modélisant le système à l'instant  $t$ , et  $H(t)$  le hamiltonien) ouvre la voie à la question du contrôle d'une telle équation. Parallèlement, il est aujourd'hui démontré expérimentalement qu'il est possible, avec un champ laser bien choisi, d'agir sur une molécule pour lui faire atteindre un état prescrit à l'avance. Cela peut par exemple permettre de favoriser, pour une molécule donnée, une voie de dissociation plutôt qu'une autre. La simulation numérique peut aider, par une procédure d'optimisation, à déterminer le champ laser approprié en fonction de la cible que l'on cherche à atteindre. Tout revient dans l'équation de Schrödinger à utiliser un hamiltonien de la forme  $H(t) = H_0 + E(t)D$ , où  $H_0$  est le hamiltonien du système moléculaire libre,  $E(t)$  la forme temporelle du champ laser et  $D$  l'opérateur moment dipolaire modélisant l'interaction entre le laser et la matière. Sur le plan mathématique, cela s'inscrit dans le contexte difficile du contrôle dit bilinéaire (le contrôle,  $E(t)D$ , multiplie l'état,  $\Psi$ ), ce qui laisse augurer d'importantes difficultés théoriques et numériques. Sur le plan numérique, la recherche d'un meilleur champ laser, ou d'une famille de champs laser convenables, se fait dans ce contexte par des algorithmes stochastiques (pour éviter les pièges créés par la multitude de minima locaux). Ces algorithmes appartiennent le plus souvent à la famille des algorithmes

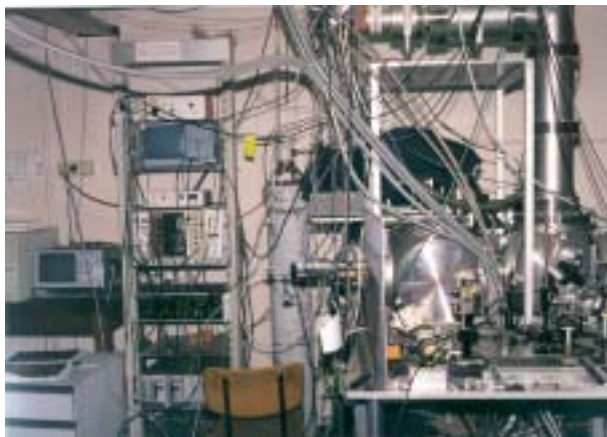


Figure 1 - Un dispositif expérimental de contrôle par laser.

génétiques. Dans ce domaine particulier où la réalisation de milliers d'expériences par minute est possible, une stratégie innovante consiste même à interfacer la boucle numérique d'optimisation avec l'expérience elle-même (plus rapide que sa simulation numérique !). En alliant modélisation physique, techniques expérimentales et simulations numériques, ce champ de la physique est en pleine explosion. Un défi scientifique en passe d'être réalisé est par exemple la réalisation d'un nanotransistor à l'échelle quantique : en actionnant le champ laser, on laisse ou non passer un micro-courant électrique à travers le système moléculaire. Une telle technologie pourrait être à la base d'une nouvelle génération d'ordinateurs.

$$\inf \{ \langle H_N \Psi, \Psi \rangle / \Psi \in L^2(\mathbf{R}^{3N}), \Psi \text{ antisymétrique, } \|\Psi\| = 1 \} \quad (2)$$

Dans ces deux formules,  $\Psi$  désigne la fonction d'onde du système et  $H_N$  le hamiltonien du problème à  $N$  corps ( $N$  désignant ici le nombre d'électrons de la molécule)

$$H_N = - \sum_{i=1}^N \Delta_{x_i} - \sum_{i=1}^N \left( \sum_{k=1}^K \frac{z_k}{|x_i - \bar{x}_k|} \right) + \sum_{1 \leq i < j \leq N} \frac{1}{|x_i - x_j|} \quad (3)$$

Dans ce hamiltonien, on a désigné par  $\bar{x}_k$  et  $z_k$  la position et la charge du  $k$ -ième des  $K$  noyaux de la molécule,

supposées connues, et par  $x_i$  la position du  $i$ -ième électron. On oublie ici, pour la simplicité de l'exposé, toutes les questions liées à la variable interne « spin » de l'électron.

Malheureusement pour la pratique numérique, le nombre d'électrons d'une molécule même petite est tel que l'on ne peut pas aborder brutalement la résolution du problème ci-dessus en raison de la complexité (exponentiellement croissante) de la discrétisation d'un espace comme  $L^2(\mathbf{R}^{3N})$ . On fait donc appel à des simplifications du problème de Schrödinger qui prennent toutes plus ou moins la forme d'un problème de minimisation du type

$$\inf \{ E(\varphi_1, \varphi_2, \dots, \varphi_N), \varphi_i \in H^1(\mathbf{R}^3), \int_{\mathbf{R}^3} \varphi_i \varphi_j = \delta_{ij} \} \quad (4)$$

où la fonctionnelle d'énergie  $E$  est dérivée de façon spécifique suivant les applications en vue pour « approcher »

l'énergie réelle au niveau Schrödinger. Les nouvelles fonctions  $\varphi_i$  recherchées (à partir desquelles on bâtera une approximation de la fonction d'onde  $\Psi$  globale du système) peuvent être pensées, *grosso modo*, comme les fonctions d'onde associées à chacun des  $N$  électrons. La plus célèbre des fonctionnelles d'énergie est celle dite de Hartree-Fock :

$$\begin{aligned}
 E(\varphi_1, \varphi_2, \dots, \varphi_N) = & \sum_{i=1}^N \int |\nabla \varphi_i|^2 \\
 & - \sum_{i=1}^N \int \left( \sum_{k=1}^K \frac{z_k}{|x - \bar{x}_k|} \right) \varphi_i^2(x) dx \\
 & + \frac{1}{2} \sum_{1 \leq i, j \leq N} \left[ \iint \frac{\varphi_i^2(x) \varphi_j^2(y)}{|x - y|} dx dy \right. \\
 & \left. - \iint \frac{\varphi_i(x) \varphi_i(y) \varphi_j(x) \varphi_j(y)}{|x - y|} dx dy \right] \quad (5)
 \end{aligned}$$

L'équation d'Euler-Lagrange associée peut se ramener à

$$H_{\varphi_1, \dots, \varphi_N} \varphi_i = \varepsilon_i \varphi_i \quad (6)$$

ce qui est en fait un système d'équations non linéaires aux valeurs propres.

La simplification apparente qui a permis de réduire la taille de l'espace à discrétiser a résulté en une complication qualitative gigantesque du problème. Partant d'un problème de minimisation quadratique (2) (ou d'une équation linéaire [1]), la stratégie a abouti à la minimisation d'une fonctionnelle d'énergie non quadratique (5), et donc à une équation d'optimalité non linéaire (6).

Du point de vue théorique, les difficultés mathématiques sont celles des problèmes de minimisation non quadratiques, souvent non convexes, posés sur des ouverts non bornés. On doit donc éviter les pertes de compacité à l'infini et autres difficultés typiques de ces problèmes. Alternativement, leur considération *via* l'équation d'Euler-Lagrange conduit à l'étude d'équations aux dérivées partielles elliptiques, non linéaires et non locales. Mathématiquement, on peut dire aujourd'hui que les caractères essentiels de ces problèmes sont bien compris. Ce constat est bien sûr un peu schématique, car certaines questions restent encore ouvertes, et l'effort constant des chimistes théoriciens pour dériver de nouvelles et meilleures approximations du problème (2) ne manquera pas de fournir de nouveaux sujets d'étude.

Du point de vue numérique, les difficultés créées par la non linéarité présente dans toutes les approximations sont en revanche aujourd'hui le sujet d'études acharnées.

## DES ALGORITHMES EFFICACES ADAPTÉS

La minimisation d'une énergie non quadratique sur un ensemble non convexe (ici essentiellement une sphère) n'est pas un exercice de calcul scientifique facile. Dans le contexte de la chimie moléculaire, les meilleurs algorithmes connus à ce jour utilisent un habile compromis entre la vision « minimisation d'une énergie » (5) et la vision « résolution de l'équation d'optimalité » (6), à savoir ici une équation non linéaire aux valeurs propres (brièvement dit, on fixe  $(\varphi_1, \dots, \varphi_N)$ , d'où la valeur de  $H_{\varphi_1, \dots, \varphi_N}$ , que l'on diagonalise pour résoudre (6), jusqu'à convergence). D'importants efforts sont en cours pour une résolution efficace à un nombre d'électrons  $N$  fixé. En fait, dans ce domaine l'objectif est double. D'abord, pour un petit nombre  $N$  d'électrons (disons moins d'une centaine), ce qui est l'apanage de l'étude théorique de la chimie des petits composés, l'objectif est de résoudre le plus précisément possible le problème. Mais aussi et surtout, un second objectif est de pouvoir aborder des nombres  $N$  grands (plusieurs milliers) pour pouvoir traiter les cas réellement intéressants pour des domaines comme la biologie et la science des matériaux. Cela se fera au prix d'approximations et de simplifications, que l'on souhaite pouvoir contrôler par une analyse numérique stricte. Dans cette optique, la donnée déterminante est la complexité algorithmique du problème. Ici, elle est particulièrement grande et parfois presque prohibitive. Disons seulement ici que, pour une méthode de type Hartree-Fock, la phase d'assemblage de la matrice (qui correspond au niveau algébrique à la transcription de la fonctionnelle d'énergie dans la base de discrétisation choisie pour les  $\varphi_i$ ) coûte un temps de l'ordre de  $N^4$ . Une fois l'assemblage effectué, la diagonalisation de la matrice coûte  $N^3$ . Il faut réaliser ces deux phases à chaque itération de l'algorithme de minimisation ou à chaque résolution de l'équation aux valeurs propres non linéaire. On comprendra que pour  $N$  grand, de tels algorithmes ne sont plus abordables. Pire, des approximations plus précises que l'approximation Hartree-Fock présentent une complexité de  $N^7$ ,  $N^8$ , voire plus.

Pour atteindre des valeurs de  $N$  pertinentes pour plus d'applications, de nombreuses pistes sont explorées. L'ambition annoncée est la construction d'algorithmes dits linéaires, c'est-à-dire dont la complexité algorithmique est de l'ordre de  $N$ .

Ainsi, l'assemblage de la matrice hamiltonienne peut se faire par des techniques dites multipôles, dans l'esprit de celles utilisées en électromagnétisme. Quant à sa diagonalisation, elle peut être évitée, au sens où le seul objet réellement nécessaire pour la détermination de l'état stationnaire est le projecteur sur les  $N$  états monoélectroniques de plus basses énergies (les  $\varphi_i$  dans [6]) et non ces états eux-mêmes. Or la détermination de ce projecteur peut se faire à un moindre frais que  $N^3$ , et sous certaines bonnes conditions, en un temps  $N$ . Une autre solution technique peut consister à développer des techniques de

type décomposition de domaine, revenant à découper le système moléculaire en différentes parties, dont on peut déterminer plus facilement l'état fondamental, puis à assembler (itérativement) les états partiels obtenus. La boucle d'itération nécessitée par la non-linéarité de (6) doit elle aussi être réalisée au plus faible coût algorithmique. Les efforts développés par la communauté sur de tels sujets sont actuellement gigantesques et font appel aux techniques les plus avancées du calcul scientifique.

### EFFETS D'ENVIRONNEMENT

Le système moléculaire que l'on désire simuler n'est bien sûr que rarement isolé. Il est le plus souvent soumis à des interactions avec son environnement. Avant tout, il peut être un constituant d'une phase condensée.

Pour simuler la présence d'une phase liquide, sujet d'étude privilégié de la chimie, une des techniques aujourd'hui la plus efficace est le couplage avec un modèle de l'échelle continue : la molécule étudiée est considérée comme le centre d'une cavité dont l'extérieur est rempli d'un continuum diélectrique de permittivité donnée. La présence de ce continuum se manifeste par la modification du potentiel coulombien d'interaction entre les charges électriques, transformant la loi d'interaction dans (3) et (5). La résolution numérique du problème fera alors appel à des méthodes intégrales, comme en électrostatique.

Pour la phase solide, cristalline par exemple, on prend en compte la répétition périodique du motif cristallin par l'intervention dans les équations du type (5) d'un paramètre « vecteur d'onde »  $\vec{k}$ . Il y aura donc une famille de problèmes du type (6) à résoudre, autant que de vecteurs  $\vec{k}$  pertinents. La célèbre théorie des bandes, expliquant la conduction des solides, est ainsi totalement explicitée dans une simulation numérique. Pour alléger le calcul, des simplifications peuvent souvent être faites, comme celle consistant à ne considérer explicitement dans le calcul que certains électrons (ceux des couches extérieures) dans chaque motif cristallin, agrégeant l'effet des autres (ceux des couches de cœur) dans des potentiels effectifs ajoutés.

Au-delà de la phase à laquelle le système moléculaire appartient, celui-ci peut subir des interactions d'autres

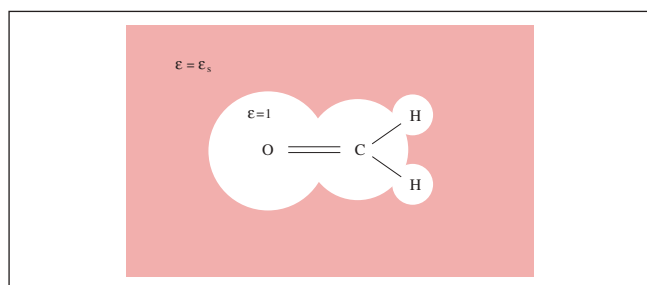


Figure 2 - Molécule plongée dans un solvant liquide.

origines : champs électriques, magnétiques... La simulation de ces interactions est par exemple un moyen de déterminer la polarisabilité d'un composé donné, son aptitude à présenter des propriétés optiques intéressantes, par exemple pour réaliser des doubleurs de fréquence (on éclaire un composé avec une fréquence  $\omega$  et la lumière transmise ressort avec une fréquence  $2\omega$ , caractéristique d'un couplage non linéaire entre la lumière et la matière à l'échelle moléculaire). Les techniques mathématiques et numériques employées dans ce cadre sont le plus souvent celles des méthodes de perturbation.

### VERS LES ÉCHELLES SUPÉRIEURES

La simulation numérique de modèles quantiques telle que nous l'avons décrite à ce stade est redoutablement précise mais, même mise en œuvre avec des méthodes numériques pointues, elle reste malheureusement limitée à ce jour à des composés de taille petite ou moyenne. Pour aborder des systèmes plus gros, composés de millions d'atomes, des simplifications sont nécessaires. La plus naturelle est de ne plus distinguer la sous-structure des atomes (électrons + noyaux) et de gérer ceux-ci comme des particules ponctuelles interagissant, *via* la mécanique newtonienne, par des champs de force. L'information de nature quantique peut être efficacement insérée dans ce modèle simplifié, par l'intermédiaire des champs de force qui peuvent être eux-mêmes précalculés par des modèles quantiques précis. Alternativement à ce couplage séquentiel, on peut aussi penser à coupler en parallèle un modèle de mécanique newtonienne avec des modèles quantiques. Ainsi, la modélisation quantique n'apparaît plus comme une discipline réservée aux petits systèmes, mais comme un moyen d'alimenter par une modélisation rigoureuse et contrôlée un niveau de description de la matière plus rudimentaire, mais aussi d'applicabilité plus large. Le célèbre champ de la dynamique moléculaire, qui est probablement le champ de la modélisation en chimie théorique ayant à ce jour le plus d'impact sur le monde expérimental et industriel (hormis les techniques de visualisation !) ne peut désormais se passer de paramètres calculés au niveau quantique ou même de couplage avec une modélisation quantique.

Du point de vue mathématique et numérique, les défis ouverts par la dynamique moléculaire ne sont pas moindres. Résoudre sur des temps longs un énorme système d'équations différentielles ordinaires

$$m_i \frac{d^2 x_i}{dt^2} = F(x_1, \dots, x_K) \quad (7)$$

présentant des échelles de temps et d'espace très disparates soulève des questions d'analyse numérique difficiles sur la symplecticité des schémas, le calcul simplifié des interactions à longue distance par schémas multi-pas, etc. C'est à ce prix que l'on peut simuler des phénomènes



## Encadré 2

# SIMULATIONS MULTI-ÉCHELLES EN SCIENCE DES MATÉRIAUX

L'arrivée de matériaux de nouvelle génération et la nécessité de pousser des matériaux existants jusqu'à leurs limites peuvent poser un problème difficile de modélisation. L'établissement de lois constitutives représentatives du comportement mécanique de ces matériaux, dans le régime d'utilisation qui va être le leur et qui est souvent éloigné du champ connu, est parfois un véritable défi. L'alternative à l'expérimentation en laboratoire est le développement de simulations numériques multi-échelles, où est décrite la manière dont comportement macroscopique du matériau et comportement de ses constituants à l'échelle microscopique sont reliés. Ainsi, pour des matériaux cristallins, on peut faire intervenir dans la simulation la façon dont les atomes constitutifs du réseau cristallin sont déplacés par le champ de déplacement macroscopique subi par le matériau et comment, en retour, le déplacement de ces atomes, influe sur le champ de contraintes présent dans le matériau. Un modèle du champ de forces à l'échelle atomique, pouvant par exemple provenir lui-même de modèles de type quantique comme ceux décrits dans le corps du texte, reliant déplacement des atomes et forces qu'ils subissent, est donc couplé avec des modèles de mécanique du continuum pour décrire l'échelle supérieure. La figure présente un exemple schématique d'un calcul numérique résultant d'une telle modélisation : en chaque point de Gauss de la triangulation utilisée pour le calcul des éléments finis, le calcul du champ de contrainte provient de l'interaction entre les atomes déplacés de leur position d'équilibre. Une démarche analogue est adoptée en mécanique

des fluides où on peut décrire la rhéologie des fluides avec micro-structures (comme les suspensions ou les fluides polymériques) à l'aide de modèles à l'échelle atomique. Dans tous les cas, l'utilisation intensive des tels modèles multi-échelles pose une foule de questions mathématiques et numériques (dérivation rigoureuse des modèles variationnels, caractère bien posé des problèmes d'évolution, convergence des schémas numériques), dont l'étude n'est aujourd'hui qu'à peine amorcée.

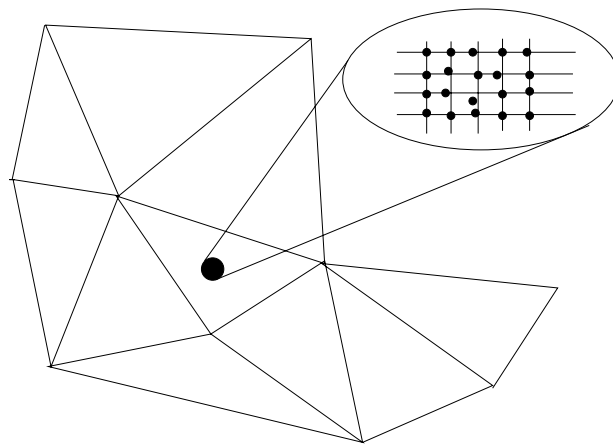


Figure - Une méthode d'éléments finis couplée à une simulation à l'échelle atomique. © Benoît Soep, LFP-CNRS

aussi complexes que le repliement d'un brin d'ADN en solution ou les dégâts causés par une cascade d'irradiation dans une structure cristalline.

## L'AVENIR

La simulation numérique en chimie moléculaire et, plus généralement, à l'échelle atomique nécessite des efforts grandissants, à l'interface de plusieurs communautés scientifiques : physiciens, chimistes, mathématiciens, numériciens, informaticiens. Elle est en route pour devenir indispensable à double titre. En premier lieu,

avec la miniaturisation des systèmes technologiques, le traitement des échelles microscopiques, voire nanoscopiques, devient une nécessité. En second lieu, la complexification des systèmes de taille usuelle et la nécessité de les comprendre dans leurs plus fins détails pour les optimiser rendent indispensable le transfert de l'information provenant de l'échelle microscopique pour mener à bien correctement les simulations effectuées aux échelles supérieures, le plus souvent macroscopiques. Dans un tel contexte, les mathématiques appliquées ont un rôle moteur à jouer.

## POUR EN SAVOIR PLUS

Cancès (E.), Le Bris (C.), « International Journal of Quantum Chemistry », Volume 79, 2000, 82.

Ciarlet (Ph.-G.), Le Bris (C.), Éditeurs, « Handbook of Numerical Analysis, special volume Computational Chemistry », Elsevier, 2003.

Defranceschi (M.), Le Bris (C.), Éditeurs, « Mathematical models and methods for ab initio Quantum Chemistry », Lecture Notes in Chemistry, volume 74, Springer, 2000.

# Un peu de géométrie des groupes

**Les groupes discrets apparaissent dans tous les domaines des mathématiques, et même chez Escher. Ils sont définis algébriquement, mais on les comprend souvent mieux en les faisant agir sur des objets géométriques. De plus en plus, on les considère comme des êtres géométriques à part entière. Leurs propriétés sont particulièrement remarquables lorsque la courbure est négative.**

## QUELQUES GROUPES

Nous considérons un groupe  $G$ , en général non commutatif (encadré). Nous le noterons multiplicativement, l'élément neutre étant noté  $1_G$  ou seulement  $1$ . Les groupes qui nous intéresseront le plus seront *de type fini*, c'est-à-dire pouvant être engendrés par un nombre fini d'éléments. Voyons quelques exemples.

- Le groupe abélien libre  $\mathbf{Z}^2$ , ou  $\mathbf{Z} \times \mathbf{Z}$ , ou  $\mathbf{Z} \oplus \mathbf{Z}$ , est l'ensemble des couples d'entiers  $(m, n)$ , avec l'addition  $(m, n) + (m', n') = (m + m', n + n')$ . Pour le noter multiplicativement, posons  $a = (1, 0)$ ,  $b = (0, 1)$ , et voyons  $\mathbf{Z}^2$  comme l'ensemble des  $a^m b^n$  muni de la multiplication  $(a^m b^n)(a^{m'} b^{n'}) = a^{m+m'} b^{n+n'}$ . L'élément neutre  $a^0 b^0$  est noté  $1$ , l'inverse de  $a^m b^n$  est  $a^{-m} b^{-n}$ .
- Considérons sur la droite réelle  $\mathbf{R}$  le groupe affine  $\text{Aff}(\mathbf{R})$  formé des homothéties et des translations, c'est-à-dire les transformations de la forme  $x \mapsto ax + b$  avec  $a, b$  réels et  $a \neq 0$ , le produit étant la composition  $(f \circ g)(x) = f(g(x))$ . C'est un groupe « continu » (groupe de Lie), mais nous pouvons considérer des sous-groupes de type fini, par exemple le groupe  $G_1$  engendré par  $t : x \mapsto x + 1$  et  $h : x \mapsto 2x$ . On vérifie que  $G_1$  est l'ensemble des transformations  $\varphi_{mnp}$  de la forme  $\varphi_{mnp}(x) = 2^m x + \frac{n}{2^p}$ , avec  $m, n, p$  entiers (encadré).
- Le groupe  $GL(n, \mathbf{R})$  des matrices  $n \times n$  à coefficients réels qui sont inversibles (c'est-à-dire de déterminant  $\neq 0$ ) est aussi un groupe de Lie. Les matrices à coefficients entiers ne forment pas un sous-groupe car le déterminant apparaît au dénominateur quand on calcule l'inverse d'une matrice. Mais  $SL(n, \mathbf{Z})$ , l'ensemble des matrices à coefficients entiers et de déterminant  $1$ , est un sous-groupe et nous considérons le

groupe  $G_2 \subset SL(2, \mathbf{Z})$  engendré par  $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$

et  $B = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ .

## GROUPES LIBRES

Dans un espace vectoriel  $V$  sur un corps  $K$ , le sous-espace vectoriel engendré par  $\{v_1, \dots, v_k\}$  est l'ensemble des combinaisons linéaires  $\sum_{i=1}^k \lambda_i v_i$ , avec  $\lambda_i \in K$ . Les éléments  $v_1, \dots, v_k$  sont indépendants si deux combinaisons linéaires différentes représentent toujours des éléments différents de  $V$  ou, de façon équivalente, s'il n'existe pas de relation  $\sum_{i=1}^k \lambda_i v_i = 0$  avec les  $\lambda_i$  non tous nuls. Le sous-espace engendré est alors de dimension  $k$ , il est isomorphe à  $K^k$ .

Dans un groupe  $G$ , le sous-groupe engendré par  $\{g_1, \dots, g_k\}$  est l'ensemble des éléments de  $G$  pouvant s'écrire comme un *mot réduit*  $g_{i_1}^{n_1} \dots g_{i_p}^{n_p}$ , où les  $n_i$  sont des entiers non nuls et  $i_j \neq i_{j+1}$ . Par exemple,  $a^2, b^{-1}c, c^{-3}a^3b^2acb^{-5}$  sont des mots en  $a, b, c$ . On prend garde de ne pas oublier le mot vide, noté  $1$ , qui représente le neutre  $1_G$ . La *longueur*  $|W|$  d'un mot  $W$  est le nombre total de lettres, en tenant compte des puissances ; ainsi  $|c^{-3}a^3b^2acb^{-5}| = 15$ .

On dira que  $g_1, \dots, g_k$  sont *indépendants* (ou forment une *famille libre*) si deux mots réduits différents représentent toujours deux éléments différents de  $G$  ou, de façon équivalente, s'il n'existe pas de relation non triviale  $g_{i_1}^{n_1} \dots g_{i_p}^{n_p} = 1$ . Ainsi la famille  $\{g\}$  (constituée du seul élément  $g$ ) est libre si et seulement si il n'y a pas de relation non triviale  $g^n = 1$ , c'est-à-dire si  $g$  est d'ordre infini. Dans les exemples ci-dessus, les familles  $\{a, b\} \subset \mathbf{Z}^2$  et  $\{h, t\} \subset G_1$  ne sont pas libres, à cause des relations  $ab = ba$  et  $hth^{-1} = t^2$ . Nous allons en revanche montrer, en utilisant la technique dite du ping-

**Encadré**

## GROUPES

Un groupe est un ensemble dans lequel on peut multiplier et inverser les éléments. Le produit doit être associatif : on a  $(xy)z = x(yz)$ , et on note simplement  $xyz$ . En revanche, le produit n'est pas forcément commutatif : on peut avoir  $xy \neq yx$ . L'inverse de  $x$  est noté  $x^{-1}$ . Il vérifie  $xx^{-1} = x^{-1}x = 1$ , où 1 désigne l'élément neutre, caractérisé par  $1x = x1 = x$ .

Par exemple, l'ensemble des permutations d'un ensemble à  $n$  éléments est un groupe fini, le groupe symétrique  $S_n$  ; le produit de deux permutations  $\sigma$  et  $\tau$  est la permutation composée, définie par  $(\sigma \circ \tau)(i) = \sigma(\tau(i))$ . Les matrices  $n \times n$  à coeffi-

cients réels qui sont inversibles (c'est-à-dire de déterminant  $\neq 0$ ) forment un groupe pour le produit matriciel.

Si  $X$  est un ensemble quelconque muni d'une certaine structure, les transformations inversibles préservant la structure forment un groupe (le produit étant toujours la composition, consistant à appliquer les transformations successivement). Si par exemple  $X$  est le plan euclidien (muni de la distance habituelle), on obtient le groupe des isométries, qui contient en particulier les rotations, les translations, les symétries orthogonales par rapport à des droites.

## SOUS-GROUPES

Une partie  $A$  d'un groupe  $G$  est un sous-groupe si c'est elle-même un groupe pour le produit de  $G$ . Il faut et il suffit pour cela que  $ab$  et  $a^{-1}$  soient dans  $A$  chaque fois que  $a$  et  $b$  y sont. Si  $A$  n'est pas un sous-groupe, il existe un plus petit sous-groupe contenant  $A$ , c'est le sous-groupe engendré par  $A$ . Lorsque le sous-groupe engendré par  $A$  est  $G$  tout entier, on dit que  $A$  engendre  $G$ . Le groupe  $G$  est de type fini s'il peut être engendré par une partie finie.

Montrons par exemple que le sous-groupe  $G_1$  engendré par  $t : x \mapsto x + 1$  et  $h : x \mapsto 2x$  dans le groupe  $\text{Aff}(\mathbf{R})$  des transformations affines de  $\mathbf{R}$  se compose des  $\varphi_{mnp}$  de la forme

$\varphi_{mnp}(x) = 2^m x + \frac{n}{2^p}$ , avec  $m, n, p$  entiers. Les formules

$$(\varphi_{mnp} \varphi_{m'n'p'})(x) = \varphi_{mnp}(\varphi_{m'n'p'}(x)) \\ = 2^{m+m'} x + \frac{2^{m+p}n' + 2^{p'}n}{2^{p+p'}} = \varphi_{m''n''p''}(x)$$

avec  $m'' = m + m'$ ,  $n'' = 2^{m+p}n' + 2^{p'}n$ ,  $p'' = p + p'$ , et  $\varphi_{mnp}^{-1} = \varphi_{m'n'p'}$  avec  $m' = -m$ ,  $n' = -n$ , et  $p' = m + p$ , montrent que l'ensemble des  $\varphi_{mnp}$  est un sous-groupe. Il contient  $h$  et  $t$ , et c'est le plus petit car  $\varphi_{mnp} = h^{-p}t^n h^{m+p}$  appartient à tout sous-groupe contenant  $h$  et  $t$ .

Si  $G$  est un groupe fini, et  $A$  est un sous-groupe, le cardinal de  $A$  divise celui de  $G$ . Le quotient est le nombre de classes de  $G$  modulo  $A$ , appelé indice de  $A$ . Ce nombre est encore défini lorsque  $G$  est infini, mais il peut être infini. S'il existe un entier  $N$  tel que, à chaque fois que l'on se donne  $g_0, g_1, \dots, g_N \in G$ , on peut trouver  $i \neq j$  avec  $g_i g_j^{-1} \in A$ , alors le plus petit de ces entiers  $N$  est l'indice de  $A$ . Sinon, l'indice de  $A$  est infini. Par exemple, l'ensemble des entiers multiples de  $d$  forme un sous-groupe de  $\mathbf{Z}$  qui est d'indice  $d$  pour  $d > 0$ , alors que  $A = \{0\}$  est d'indice infini.

pong, que les matrices  $A$  et  $B$  sont indépendantes dans  $SL(2, \mathbf{Z})$ .

Pour cela, faisons agir  $SL(2, \mathbf{Z})$  sur  $P = \mathbf{R} \cup \{\infty\}$  (la droite projective réelle) en associant à  $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

l'homographie  $h_M : x \rightarrow \frac{ax + b}{cx + d}$  (avec les conventions

usuelles, en particulier  $h_M\left(-\frac{d}{c}\right) = \infty$  et  $h_M(\infty) = \frac{a}{c}$

si  $c \neq 0$ ). La définition est faite pour que  $h_{MN} = h_M h_N$ .

Soit  $P_A = ]-1, 1[$ , et soit  $P_B$  le complémentaire de  $]-1, 1[$ . On a  $h_A(x) = x + 2$  et par conséquent  $h_A^n(P_A) \subset P_B$  pour tout  $n \neq 0$ . On a de même

$h_B(x) = \frac{x}{2x + 1}$  et  $h_B^n(P_B) \subset P_A$  pour  $n \neq 0$ . Nous

allons maintenant jouer au ping-pong avec  $P_A$  et  $P_B$ .

Pour montrer l'indépendance de  $A$  et  $B$ , considérons un mot réduit non trivial, par exemple  $W = B^2 A B^{-3} A^5$ . Appliquons  $h_W = h_B^2 h_A h_B^{-3} h_A^5$  à  $P_A$ . L'élément  $h_A^5$  l'envoie dans  $P_B$ , l'élément  $h_B^{-3}$  le renvoie dans  $P_A$ , etc. et finalement  $h_W(P_A)$  est contenu dans  $P_A$ , sans lui être égal. Cela empêche  $h_W$  d'être l'identité et donc  $W$  d'être égal à 1 dans  $SL(2, \mathbf{Z})$ , cqfd. Ce raisonnement s'applique à tout mot  $W$  commençant par une puissance de  $B$  et se terminant par une puissance de  $A$ . Les autres cas se traitent de manière analogue : si  $W$  commence et se termine par une puissance de  $A$ , on a  $h_W \neq id$  car

$h_W(P_A) \subset P_B$  ; si  $W$  se termine par une puissance de  $B$ , on applique  $h_W$  à  $P_B$ .

Puisque  $A$  et  $B$  sont indépendants, tout élément de  $G_2$  s'écrit de façon unique comme un mot réduit en  $A$  et  $B$ . A ce point, on peut oublier que  $A$  et  $B$  sont des matrices, et voir  $G_2$  comme l'ensemble  $F(A, B)$  des mots réduits en deux symboles abstraits  $A$  et  $B$ . La multiplication consiste à juxtaposer et réduire ; par exemple  $(B^2AB^{-3}A^5)(A^{-5}BA^4) = B^2AB^{-2}A^4$ , et l'inverse de  $B^2AB^{-3}A^5$  est  $A^{-5}B^3A^{-1}B^{-2}$ . On dit que  $G_2$  est le groupe libre de rang 2, souvent noté  $F_2$ . On définit de même  $F_n$ , le groupe libre de rang  $n$ , pour  $n > 2$ .

Beaucoup de groupes contiennent des groupes libres. On montre par exemple que deux rotations de la sphère prises au hasard engendrent un groupe libre, les transformations  $x \mapsto x + 1$  et  $x \mapsto x^3$  sur  $\mathbf{R}$  aussi.

Le groupe  $F_2$  contient des familles libres arbitrairement grandes : on voit facilement que la famille infinie  $\{A^n B A^{-n}\}_{n \in \mathbf{N}}$  est libre, car les  $B$  ne se simplifient pas quand on multiplie ces éléments. Le groupe libre de rang 2 contient donc des groupes libres de rang quelconque et même des groupes qui ne sont pas de type fini. Le théorème de Nielsen-Schreier garantit que tout sous-groupe d'un groupe libre est libre, c'est-à-dire qu'il est engendré par une famille libre.

L'ALTERNATIVE DE TITS

Nous avons déjà remarqué que  $G_1$  n'est pas libre, car ses générateurs vérifient  $hth^{-1} = t^2$ . Pour obtenir d'autres relations, remarquons que dans  $\text{Aff}(\mathbf{R})$ , et donc dans  $G_1$ , tout commutateur  $[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}$  est une translation, et que deux translations commutent. On a donc  $[g_1, g_2][g_3, g_4] = [g_3, g_4][g_1, g_2]$  pour tous  $g_1, g_2, g_3, g_4 \in G_1$ . Cette relation « universelle » exprime que  $G_1$  est métabelien, ou encore résoluble de classe 2.

Plus généralement, on dit que  $G$  est résoluble de classe  $\leq p$  si le sous-groupe engendré par tous les commutateurs  $[g_1, g_2]$  est résoluble de classe  $\leq p - 1$ , c'est-à-dire si  $2^p$  éléments quelconques de  $G$  vérifient une certaine identité formée à partir de commutateurs itérés. Les groupes résolubles sont ceux que l'on peut obtenir par extensions à partir de groupes commutatifs. La non-résolubilité par radicaux des équations algébriques de degré 5 est due à la non-résolubilité du groupe symétrique  $S_5$  (théorie de Galois).

On vérifie facilement que, pour tout corps  $K$ , le sous-groupe de  $GL(n, K)$  formé des matrices triangulaires supérieures inversibles est résoluble (de classe  $n$ ). La célèbre alternative de Tits (1972) affirme que, si le groupe de type fini  $G$  est linéaire, c'est-à-dire isomorphe à un sous-groupe d'un  $GL(n, K)$ , alors ou bien  $G$  contient un sous-groupe isomorphe à  $F_2$ , ou bien un sous-groupe d'indice fini de  $G$  (encadré) est résoluble. Autrement dit,

ou bien  $G$  contient des familles libres arbitrairement grandes, ou bien (à indice fini près) les éléments de  $G$  vérifient une relation universelle. L'alternative de Tits a été étendue à d'autres groupes ; ainsi Bestvina, Feighn et Handel l'ont récemment montrée pour les sous-groupes du groupe  $Out(F_n)$  des automorphismes d'un groupe libre de rang fini, modulo les conjugaisons.

RELATIONS ET PRÉSENTATIONS

Si un groupe  $G$  n'est pas libre, des mots réduits différents peuvent représenter le même élément : on dit qu'ils sont équivalents. Le problème du mot consiste à décider (algorithmiquement) si deux mots donnés sont ou non équivalents. Il suffit en fait de savoir décider quels mots sont triviaux, c'est-à-dire représentent l'élément neutre  $1_G$ .

C'est facile dans  $\mathbf{Z}^2$ , qui est commutatif. Il est par exemple immédiat pour nous que  $a^{100}b^{100}a^{-100}b^{-100} = 1$ . Mais une machine qui ne saurait qu'appliquer mécaniquement la relation de base  $ab = ba$  (et, soyons généreux, les relations  $a^{\pm 1}b^{\pm 1} = b^{\pm 1}a^{\pm 1}$ ) trouverait pénible de montrer cette égalité : il lui faudrait en effet faire passer séparément chacun des cent  $a^{-1}$  à gauche de chaque  $b$ , soit 10 000 opérations pour un mot de longueur 400. De manière générale, le nombre d'opérations nécessaires pour montrer la trivialité d'un mot de longueur  $n$  est, dans le pire des cas, de l'ordre de  $n^2$  pour  $n$  grand. On parle pour  $\mathbf{Z}^2$  d'inégalité isopérimétrique quadratique.

L'interprétation géométrique est la suivante (figure). Quadrillons le plan par un grillage dont les barreaux horizontaux sont orientés vers la droite et portent la lettre  $a$ , les barreaux verticaux étant orientés vers le haut et portant  $b$ . Fixons un sommet  $E$  de ce graphe comme origine.

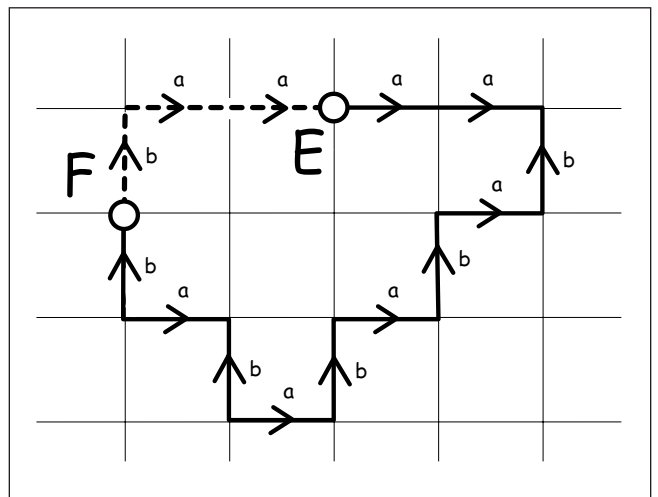


Figure 1 - Les mots  $a^2b^{-1}a^{-1}b^{-1}a^{-1}b^{-1}a^{-1}ba^{-1}b$  et  $a^{-2}b^{-1}$  représentent le même élément de  $\mathbf{Z}^2$  : les chemins associés ont la même extrémité F.

Un mot en  $a$  et  $b$  se représente alors comme un chemin issu de  $E$ , par exemple  $a^2b^{-1}a^{-1}b^{-1}$  fait aller deux unités vers la droite, une vers le bas, une vers la gauche et une vers le bas.

On remarque que deux mots sont équivalents si et seulement si les chemins associés ont la même extrémité : par exemple  $a^2b^{-1}a^{-1}b^{-1}a^{-1}b^{-1}a^{-1}ba^{-1}b$  est équivalent à  $a^{-2}b^{-1}$ . En particulier, les sommets du graphe s'identifient avec les éléments de  $\mathbf{Z}^2$  et un mot est trivial si et seulement si le chemin associé est un lacet (il se referme en  $E$ ). Ainsi  $a^{100}b^{100}a^{-100}b^{-100}$  représente le bord d'un carré de côté 100. Appliquer la relation  $a^{\pm 1}b^{\pm 1} = b^{\pm 1}a^{\pm 1}$  revient à faire traverser au lacet une maille du grillage, et 10 000 est simplement l'aire du carré.

L'exposant 2 obtenu plus haut est ainsi celui par lequel s'exprime l'aire d'un carré en fonction de son côté. On voit l'analogie avec l'inégalité isopérimétrique classique majorant l'aire bordée par une courbe plane par le carré de sa longueur (divisé par  $4\pi$ , mais peu importe ici).

Revenant à l'algèbre, nous allons maintenant expliquer comment résoudre le problème du mot dans  $G_1$  en utilisant uniquement la relation  $hth^{-1}t^{-2} = 1$ . Grâce aux équations  $ht^{\pm 1} = t^{\pm 2}h$  et  $t^{\pm 1}h^{-1} = h^{-1}t^{\pm 2}$ , on peut dans un mot faire passer toutes les puissances positives de  $h$  à la droite du mot et toutes les puissances négatives à gauche. En d'autres termes, un mot quelconque  $W$  est équivalent dans  $G_1$  à un mot de la forme  $h^{-m}t^n h^p$  avec  $m, p \geq 0$ . Un tel mot représente la transformation  $x \mapsto 2^{p-m}x + 2^{-m}n$ , qui est l'identité si et seulement si  $n = 0$  et  $p = m$ , c'est-à-dire si le mot est vide. Donc  $W = 1$  dans  $G_1$  si et seulement si le mot  $h^{-m}t^n h^p$  associé à  $W$  est le mot vide : le problème du mot est résolu.

Ce raisonnement montre en fait que toutes les relations vérifiées par  $h$  et  $t$  se déduisent formellement de la relation  $hth^{-1}t^{-2} = 1$ . On dit que  $G_1$  est présenté par les éléments  $h$  et  $t$  soumis à la relation  $hth^{-1}t^{-2} = 1$ .

De manière générale, on dit que

$$G = \langle g_1, \dots, g_k^{-1} / r_1, \dots, r_q \rangle,$$

où les  $r_j$  sont des mots en les  $g_i$ , est une présentation de  $G$  si  $G$  est engendré par des éléments  $g_i$  vérifiant les relations  $r_j = 1$ , et si toute relation entre les  $g_i$  se déduit formellement des relations  $r_j = 1$  (plus précisément,  $G$  est isomorphe au quotient du groupe libre  $F(g_1, \dots, g_k)$  par le sous-groupe formé des produits de conjugués des  $r_j$  et de leurs inverses).

Fixons un entier  $m$  et demandons maintenant à une machine de montrer la relation  $[h^m t h^{-m}, t] = 1$  à partir de  $hth^{-1}t^{-2} = 1$ . C'est facile pour nous, qui pouvons voir que  $h^m t h^{-m} = t^{2^m}$ . Mais pour la machine, le nombre d'opérations sera de l'ordre de  $2^m$ , donc une fonction exponentielle de la longueur de  $[h^m t h^{-m}, t]$  (égale à  $4m + 4$ ). Les mots  $[h^m t h^{-m}, t]$  étant représentatifs du cas général,  $G_1$  vérifie une *inégalité isopérimétrique exponentielle*.

## LA FONCTION DE DEHN

Étant donné une présentation finie

$$G = \langle g_1, \dots, g_k^{-1} / r_1, \dots, r_q \rangle,$$

nous allons définir la *fonction de Dehn*  $\varphi(n)$ , dont la croissance détermine l'inégalité isopérimétrique vérifiée par  $G$ . Un remplacement tel que  $a^{\pm 1}b^{\pm 1} \mapsto b^{\pm 1}a^{\pm 1}$  ou  $ht^{-1} \mapsto t^{\pm 2}h$  revient à multiplier le mot par un conjugué d'un  $r_j^{\pm 1}$ , et un mot  $W$  est trivial dans  $G$  si et seulement si dans le groupe libre  $F(g_1, \dots, g_k)$  on peut écrire  $W = \prod_{m=1}^s u_m r_{j_m}^{\pm 1} u_m^{-1}$ . Pour chaque mot trivial  $W$ , on considère le plus petit  $s$  possible, et  $\varphi(n)$  est le maximum de ces  $s$  pour tous les mots triviaux de longueur  $\leq n$ .

La fonction de Dehn dépend de la présentation, mais la manière dont elle croît (quadratique, exponentielle, etc.) ne dépend que de  $G$ . Nous avons dit que  $\varphi$  est quadratique pour  $\mathbf{Z}^2$  et exponentielle pour  $G_1$  ; voici un exemple de  $\varphi$  linéaire.

Soit  $G_3$  le groupe de présentation  $\langle a, b, c, d / aba^{-1}b^{-1}cdc^{-1}d^{-1} \rangle$  (groupe fondamental de la surface fermée orientable de genre 2). Étant donné un mot  $W$  en  $a, b, c, d$ , nous pouvons le raccourcir s'il contient plus de la moitié de la relation, ou de son inverse, à permutation circulaire près. On peut ainsi remplacer  $aba^{-1}b^{-1}c$  par  $dcd^{-1}$ ,  $d^{-1}c^{-1}bab^{-1}$  par  $c^{-1}d^{-1}a$ ,  $dc^{-1}d^{-1}ab$  par  $c^{-1}ba$ , etc. On réduit alors le mot obtenu (si l'on peut) et on recommence autant que possible.

Dehn a montré (vers 1910) que dans  $G_3$  cet algorithme, dit *algorithme de Dehn*, résout le problème du mot :  $W$  représente 1 si, mais surtout *seulement si*, l'algorithme aboutit au mot vide. La longueur du mot diminuant à chaque itération, le nombre d'opérations est majoré par la longueur du mot :  $G_3$  vérifie une *inégalité isopérimétrique linéaire*.

Les groupes dans lesquels le problème du mot se résoud par l'algorithme de Dehn (raccourcir le mot s'il contient plus de la moitié d'une relation) ont une fonction de Dehn au plus linéaire. Réciproquement, on montre qu'un groupe à fonction de Dehn au plus linéaire admet une présentation pour laquelle l'algorithme de Dehn s'applique. Ces groupes sont en fait les *groupes hyperboliques* définis par Gromov vers 1985 ; nous évoquons ci-dessous leurs aspects géométriques.

Si  $G$  n'est pas hyperbolique, on montre que sa fonction de Dehn est au moins quadratique. Il n'y a en revanche pas de trou au-delà de l'exposant 2 : Brady et Bridson ont récemment montré que l'ensemble des  $\alpha$  tels qu'il existe un groupe de fonction de Dehn équivalente à  $n^\alpha$  est dense dans  $[2, +\infty[$  (on notera que l'ensemble des classes d'isomorphisme de groupes de présentation finie est dénombrable, donc l'ensemble de ces  $\alpha$  aussi).

Connaître explicitement la fonction de Dehn d'un groupe de présentation finie permet la résolution algo-

rithmique du problème du mot dans ce groupe : pour savoir si un mot  $W$  de longueur  $n$  est trivial, il suffit de le comparer à toutes les expressions  $\prod_{m=1}^s u_m r_{j_m}^{\pm 1} u_m^{-1}$  avec  $s \leq \varphi(n)$ , qui sont en nombre fini (la longueur des mots  $u_m$  peut être bornée *a priori*). Inversement, un algorithme résolvant le problème permet de calculer  $\varphi$ .

On sait qu'il existe des groupes de présentation finie dans lesquels le problème du mot ne peut pas être résolu algorithmiquement, car la fonction de Dehn n'est pas récursive : elle croît tellement vite qu'aucun algorithme ne peut la calculer. Donc en toute généralité, on ne peut rien dire d'un groupe donné par générateurs et relations (même pas savoir si le groupe est trivial ou non...). Mais le plus souvent, toute information algébrique ou géométrique sur  $G$ , même minime, permet de l'analyser.

### LE PLAN HYPERBOLIQUE $H^2$

Regardons par exemple le groupe  $G_3$  d'un point de vue géométrique (comme le faisait Dehn). Essayons de construire un graphe comme pour  $Z^2$ . Le graphe à considérer n'est plus de degré 4, mais de degré 8 : de chaque sommet partent 4 arêtes étiquetées  $a, b, c, d$  et il en arrive 4. Les mailles du grillage sont des octogones, correspondant à la relation  $aba^{-1}b^{-1}cdc^{-1}d^{-1}$ . On peut essayer de dessiner ce graphe, mais on manque très vite de place pour tracer 8 arêtes en chaque sommet : on ne peut pas paver le plan par des octogones réguliers. Ce graphe doit en fait être tracé non dans le plan euclidien mais dans le plan hyperbolique  $H^2$ .

Imaginons une piscine circulaire (plus mathématiquement, le disque unité ouvert  $D$  dans le plan) remplie d'un liquide visqueux, d'autant plus dense que l'on s'approche du bord : le coefficient de viscosité est proportionnel à  $\frac{1}{1-r^2}$ , où  $r$  est la distance euclidienne au centre du disque. On définit la distance (hyperbolique !) entre deux points  $x, y$  de  $D$  comme le temps nécessaire au lecteur pour nager de  $x$  à  $y$ .

Il existe toujours un plus court chemin de  $x$  à  $y$  (appelé géodésique), mais il ne nous apparaît pas comme rectiligne : il s'incurve vers le centre du disque pour pouvoir aller plus vite, tout comme un avion prend de l'altitude pour réduire la résistance de l'air. Les géodésiques sont en fait les arcs contenus dans des cercles perpendiculaires au bord de  $D$ , ainsi que les diamètres (noter que le bord de  $D$  est « à l'infini », on ne peut pas l'atteindre en un temps fini).

Comme le plan euclidien, le plan hyperbolique est un espace métrique homogène : on peut envoyer tout point sur tout autre point par une isométrie (en particulier, le « centre » de  $D$  ne joue pas un rôle particulier ; toute homographie du plan complexe qui envoie  $D$  sur lui-même induit une isométrie). Mais il est à courbure négative,

alors que le plan euclidien est à courbure nulle et la sphère à courbure positive.

Escher a utilisé des pavages de  $H^2$  par exemple, « Limite circulaire III » (figure 2) évoque un pavage par des triangles et quadrilatères réguliers, séparés par des lignes blanches géodésiques.



Figure 2 - Le plan hyperbolique vu par M.C. Escher.

Pour étudier  $G_3$ , on pave  $H^2$  par des octogones réguliers dont les côtés sont des segments géodésiques de même longueur et dont les angles valent  $2\pi/8$  (soit  $45^\circ$ ), de façon que 8 octogones se touchent en chaque sommet. Le graphe associé à un tel pavage est le « grillage » cherché pour  $G_3$ .

La fonction de Dehn de  $G_3$  est ainsi linéaire car  $H^2$  vérifie une inégalité isopérimétrique linéaire : on peut borner l'aire bordée par une courbe par une fonction linéaire de sa longueur. Par exemple, un disque de rayon  $R$  est d'aire  $2\pi sh R$ , comparable à son périmètre  $2\pi(ch R - 1)$  (il vaut mieux faire des puzzles dans le plan hyperbolique : quand on a posé le bord, on a placé une proportion non négligeable des pièces).

La géométrie élémentaire dans  $H^2$  réserve d'autres surprises. Ainsi, l'axiome des parallèles d'Euclide n'est pas vrai et la somme des angles d'un triangle ne vaut pas  $\pi$  (=  $180^\circ$ ) : elle est égale à  $\pi$  moins l'aire du triangle (en particulier, l'aire d'un triangle est au plus  $\pi$ ).

Une autre propriété fondamentale de  $H^2$  est la finesse des triangles : il existe une constante  $\delta$  (égale à  $\log(\sqrt{2} + 1)$ ) telle que tout point situé sur un côté d'un triangle à bords géodésiques est à distance au plus  $\delta$  d'un point situé sur l'un des deux autres côtés. Cette propriété s'appelle  $\delta$ -hyperbolicité ou simplement hyperbolicité.

## GROUPES HYPERBOLIQUES ET QUASI-ISOMÉTRIES

Nous avons vu que le groupe  $\mathbf{Z}^2$  « ressemble » au plan euclidien, alors que  $G_3$  « ressemble » au plan hyperbolique. Suivant Gromov, on formalise cela en regardant un groupe  $G$ , muni d'un système fini  $S$  de générateurs, comme un espace métrique : la distance entre deux éléments  $g$  et  $h$  de  $G$  est la longueur minimale d'un mot (écrit avec les éléments de  $S$ ) représentant  $g^{-1}h$ .

On visualise mieux cet espace « discret » en le considérant comme l'ensemble des sommets du *graphe de Cayley* de  $G$  : on place une arête entre deux sommets  $g, h$  si  $h$  s'obtient à partir de  $g$  par multiplication à droite par un élément de  $S$ , et on décide que chaque arête est un segment de longueur 1. La distance entre deux points est simplement celle d'un chemin de longueur minimale les joignant (un tel chemin s'appelle encore géodésique).

Le graphe de Cayley du groupe libre  $G_2$  est un arbre (il n'y a pas de boucle). Celui de  $\mathbf{Z}^2$  est le grillage utilisé plus haut, avec la distance dite du chauffeur de taxi new-yorkais (noter qu'il existe en général plusieurs géodésiques entre deux points donnés). Cette distance n'est pas celle du plan euclidien (qui est le vol d'oiseau), mais elle lui est comparable : le rapport des deux distances est compris entre deux constantes strictement positives (ici 1 et  $\sqrt{2}$ ). De même, le graphe de  $G_3$  est formé des géodésiques délimitant les octogones du pavage de  $H^2$  mentionné plus haut, avec une distance comparable à la distance hyperbolique.

On dit que  $G$  est un *groupe hyperbolique* s'il existe une constante  $\delta$  telle que son graphe de Cayley soit  $\delta$ -hyperbolique, c'est-à-dire si les triangles du graphe de Cayley, comme ceux de  $H^2$ , sont fins. Ainsi  $G_2$  et  $G_3$  sont hyperboliques,  $\mathbf{Z}^2$  ne l'est pas ( $G_1$  non plus).

Pour présenter nos exemples, nous avons toujours choisi le système de générateurs évident, le plus simple. Mais un groupe de type fini possède une infinité de systèmes générateurs, donc une infinité de graphes de Cayley différents, et il n'est pas évident qu'ils soient tous hyperboliques si l'un d'entre eux l'est.

En fait, tous ces graphes se ressemblent, de même qu'ils ressemblent à l'espace discret  $G$  considéré plus haut, tout comme le graphe de Cayley de  $\mathbf{Z}^2$  ressemble au plan euclidien et celui de  $G_3$  à  $H^2$ , la ressemblance devant être comprise comme une *quasi-isométrie*.

Deux espaces métriques  $X, Y$  sont quasi isométriques s'il existe une application  $f : X \rightarrow Y$  et une constante  $\lambda > 1$ , telle que  $f$  ne distord pas trop les distances des points assez éloignés (le rapport entre  $d_Y(f(x), f(x'))$  et  $d_X(x, x')$  est compris entre  $\frac{1}{\lambda}$  et  $\lambda$  si  $d_X(x, x') > \lambda$ ) et  $f$  est presque surjective (toute boule de rayon  $\lambda$  dans  $Y$  contient un point de l'image).

Tout espace borné est quasi isométrique à un point, la quasi-isométrie est faite pour capturer des propriétés à l'infini (on dit *asymptotiques*) des espaces. Deux espaces (géodésiques) quasi isométriques sont simultanément hyperboliques ou non, ce qui légitime la définition d'un groupe hyperbolique donnée ci-dessus.

A un groupe de type fini est ainsi associé un espace métrique, bien défini à quasi-isométrie près. On peut en particulier parler de groupes quasi isométriques entre eux. Beaucoup de propriétés algébriques ou géométriques des groupes sont invariantes par quasi-isométrie : par exemple être fini, de présentation finie, contenir un sous-groupe commutatif d'indice fini, être hyperbolique, avoir une fonction de Dehn avec un type de croissance donné. De manière générale, on cherche à classer les groupes à quasi-isométrie près.

Mentionnons simplement un récent résultat de rigidité dû à Farb et Mosher. Pour  $n$  entier  $\geq 2$ , soit  $H_n$  le sous-groupe de  $\text{Aff}(\mathbf{R})$  engendré par  $x \mapsto x + 1$  et  $x \mapsto nx$  ( $H_2$  est donc le  $G_1$  étudié plus haut). Si  $n$  est une puissance de  $m$ , alors  $H_n$  est un sous-groupe d'indice fini de  $H_m$ , il lui est donc quasi isométrique. Inversement, Farb et Mosher ont montré que  $H_n$  et  $H_m$  sont quasi isométriques si et seulement si  $n$  et  $m$  sont des puissances d'un même entier, et (essentiellement) qu'un groupe de type fini quasi isométrique à un  $H_n$  contient un sous-groupe d'indice fini isomorphe à un  $H_{n^p}$ .

### POUR EN SAVOIR PLUS

**Gersten (S.)**, Introduction to hyperbolic and automatic groups, Summer School in Group Theory in Banff, 1996, 45-70, CRM Proc. *Lecture Notes*, 17, Amer. Math. Soc., Providence, RI, 1999.

**Ghys (E.), de la Harpe (P.) (éditeurs)**, Sur les groupes hyperboliques d'après Mikhael Gromov, *Progress in Mathematics* 83, Birkhäuser.

**Glass (A.)**, The ubiquity of free groups, *Math. Intelligencer* 14, n° 3, 54-57, 1992.

**Valette (A.)**, Quelques coups de projecteurs sur les travaux de Jacques Tits, *Gazette des Mathématiciens* n° 61, 61-79, 1994.

# Mathématiques et turbulence

*En ce début de millénaire, la « turbulence » est l'une des grandes questions fondamentales qui reste sur le métier du physicien. De leur côté, d'éminents mathématiciens ont distingué la résolution des équations de Navier-Stokes comme l'un des problèmes clé pour l'avenir de leur discipline. Quel est le lien entre les préoccupations des uns et des autres ? C'est ce que je me propose d'examiner ici.*

Comme tous les mathématiciens ne sont pas forcément familiers avec la mécanique des fluides, je vais commencer par les quelques généralités d'usage.

## L'OBJET DE LA MÉCANIQUE DES FLUIDES

Le but de la mécanique des fluides est de décrire et calculer les différents types d'écoulements fluides que nous pouvons observer. La difficulté de cette entreprise apparaît immédiatement en faisant une expérience simple (et qui ne coûte pas cher).

Observons la fumée d'une cigarette montant dans l'air calme : que voit-on ? Sur quelques dizaines de centimètres, la fumée s'élève tranquillement et les particules de fumée nous paraissent suivre des trajectoires régulières, sensiblement parallèles, qu'elles décrivent de manière uniforme ; puis sur une dizaine de centimètres environ, cet ordonnancement se disloque au profit de quelques tourbillons d'une taille comparable à la largeur de la colonne de fumée ; ils évoluent et se déforment en s'élevant pour brusquement laisser place à un mouvement tellement désordonné qu'on ne peut plus suivre à l'œil la trajectoire d'une particule.

Dans la zone basse, l'écoulement ordonné est appelé laminaire ; dans la plus haute, il est dit turbulent, tandis que la zone intermédiaire est baptisée zone de transition.

Dans ces trois zones, les conditions dans lesquelles s'effectue l'écoulement sont voisines et pourtant, les comportements sont très différents. Si l'on admet que ces mouvements sont représentés par une même équation cela laisse présager que la résolution de cette équation va donner du fil à retordre.

La connaissance des deux premiers régimes a fait des progrès si considérables au cours du  $xx^e$  siècle que l'on peut les considérer comme bien connus ; le troisième en revanche demeure une énigme.

## LES ÉQUATIONS D'EULER ET NAVIER-STOKES

La première équation décrivant le mouvement d'un milieu continu fluide a été écrite par Euler en 1755 : c'est l'équation (ou plutôt les équations) du fluide parfait (sans frottement interne).

Sous leur forme la plus usuelle, les équations du mouvement (équations d'Euler) pour un fluide parfait incompressible, occupant un domaine  $\Omega$  de l'espace, s'écrivent :

$$(E) \quad \begin{cases} \frac{\partial \mathbf{u}}{\partial t} + (\mathbf{u} \cdot \nabla) \mathbf{u} = -\nabla p \\ \operatorname{div} \mathbf{u} = 0 \end{cases}$$

où  $\mathbf{u}(t, \mathbf{x})$  est le champ de vitesse du fluide et  $p(t, \mathbf{x})$  sa pression. A ces équations, il faut ajouter une condition limite pour la vitesse au bord  $\partial\Omega$  du domaine :  $\mathbf{u} \cdot \mathbf{n} = 0$  ( $\mathbf{n}$  désigne le vecteur normal unitaire sortant au bord du domaine). Pour déterminer complètement le mouvement du fluide, il nous faudra en outre fixer une condition initiale  $\mathbf{u}_0(\mathbf{x})$  (i.e. résoudre le problème de Cauchy).

Il est assez piquant de noter que c'est (avec celle des cordes vibrantes) la première EDP de physique mathématique qui ait été écrite, et elle résiste encore...

Il a fallu ensuite un certain temps avant que l'on sache modéliser le frottement interne, et l'équation du fluide visqueux (équation de Navier-Stokes) a été obtenue par Navier en 1824. Elle s'écrit (en supposant toujours le fluide incompressible, de masse volumique constante égale à 1) :

$$(N-S) \quad \begin{cases} \frac{\partial \mathbf{u}}{\partial t} + (\mathbf{u} \cdot \nabla) \mathbf{u} - \nu \Delta \mathbf{u} = -\nabla p, \text{ sur } \Omega \\ \operatorname{div} \mathbf{u} = 0 \end{cases}$$



Le paramètre  $\nu$  est la viscosité cinématique (normalisée par la masse volumique) du fluide et il faut bien sûr rajouter une condition au bord du domaine, la plus couramment employée étant celle de Stokes  $\mathbf{u} = 0$  sur  $\partial\Omega$ . Il faut également fixer la condition initiale  $\mathbf{u}_0(\mathbf{x})$ .

Une fois ces équations écrites, venons-en à une caractéristique physique importante des écoulements : le **nombre de Reynolds**.

Dans l'équation de N-S, le terme  $(\mathbf{u} \cdot \nabla)\mathbf{u}$  est appelé terme convectif : c'est un terme non linéaire générateur d'instabilités et c'est lui qui est tenu pour responsable de l'aspect turbulent lorsqu'il advient ; le terme  $\nu \Delta \mathbf{u}$  est le terme visqueux ; il a l'effet contraire de lisser l'écoulement et de lui donner un caractère laminaire. C'est l'ordre de grandeur du rapport entre ces deux termes qui va conditionner l'aspect de l'écoulement. On définit ainsi le nombre (sans dimension) de Reynolds de l'écoulement :

$$\text{Re} = \frac{|(\mathbf{u} \cdot \nabla)\mathbf{u}|}{|\nu \Delta \mathbf{u}|} \approx \frac{UL}{\nu},$$

où  $L$  et  $U$  sont respectivement des longueur et vitesse caractéristiques de l'écoulement.

L'observation expérimentale nous dit maintenant qu'il existe un nombre de Reynolds critique  $\text{Re}^*$  tel que, pour  $\text{Re} < \text{Re}^*$ , l'écoulement soit laminaire, et turbulent pour  $\text{Re} > \text{Re}^*$ . Évidemment,  $\text{Re}^*$  n'est pas universel ; il va dépendre de la géométrie du domaine et du type de condition initiale... mais disons qu'en gros il est de l'ordre de 100.

Sachant que pour l'air la viscosité cinématique est de  $0,15 \text{ cm}^2/\text{s}$ , on peut tout de suite obtenir quelques ordres de grandeur.

Écoulement autour d'une automobile :

$$\text{Re} \approx 10^7 \quad (U = 100 \text{ km/h}, L = 4\text{m}).$$

Écoulement météorologique :

$$\text{Re} \approx 10^{12} \quad (U = 10 \text{ m/s}, L = 1000 \text{ km}).$$

Vol d'une mouche :

$$\text{Re} \approx 300 \quad (U = 1 \text{ m/s}, L = 0,5 \text{ cm}).$$

On voit donc que la plupart des écoulements qui se situent à notre échelle sont pleinement turbulents ; la mouche, elle, évolue constamment dans la zone de transition laminaire-turbulent, ce qui doit certainement lui poser des problèmes de contrôle de vol tout à fait intéressants ; *idem* pour la fumée de cigarette, ce qui explique que l'on puisse observer les trois régimes simultanément.

Il est commode d'écrire les équations de N-S de manière adimensionnée (en faisant les changements d'échelle appropriés) ; on obtient alors :

$$\frac{\partial \mathbf{u}}{\partial t} + (\mathbf{u} \cdot \nabla)\mathbf{u} - \frac{1}{\text{Re}} \Delta \mathbf{u} = -\nabla p.$$

## MATHÉMATIQUE DES ÉQUATIONS DE NAVIER-STOKES ET EULER

L'essentiel de ce que l'on sait sur la résolution du problème de Cauchy pour les équations N-S, avec une donnée initiale  $\mathbf{u}_0(\mathbf{x})$ , dans un domaine borné  $\Omega$  de  $\mathbb{R}^3$ , remonte aux travaux de Leray (1933-34).

**Théorème.** *Si  $\mathbf{u}_0(\mathbf{x})$  est suffisamment régulière sur  $\overline{\Omega}$  et vérifie  $\text{div } \mathbf{u}_0 = 0$ ,  $\mathbf{u}_0 = 0$  sur  $\partial\Omega$ , il existe une solution classique unique pendant un intervalle de temps  $[0, T^*]$ . Au-delà de  $T^*$ , il existe une solution moins régulière (solution faible) dont on ne sait pas montrer l'unicité.*

L'énoncé volontairement un peu vague de ce résultat appelle quelques commentaires.

– Par « suffisamment régulière » on entend que  $\mathbf{u}$  ainsi que son gradient (pris au sens des distributions) sont de carré intégrable sur  $\Omega$ .

– Le temps  $T^* > 0$  dépend bien sûr de  $\mathbf{u}_0(\mathbf{x})$  ; il est d'autant plus petit que  $\mathbf{u}_0$  est « grand ».

– Sens de la notion de solution faible. Si  $\mathbf{u}$  n'est pas régulier, le terme  $(\mathbf{u} \cdot \nabla)\mathbf{u}$  n'a, *a priori*, pas de sens. On peut lui en donner un : en utilisant la condition  $\text{div } \mathbf{u} = 0$ , on voit que pour  $\mathbf{u}$  régulier  $(\mathbf{u} \cdot \nabla)\mathbf{u} = \partial_i(u_i \mathbf{u})$  et que cette dernière expression existe au sens des distributions dès que  $\mathbf{u}$  est de carré intégrable. Il suffit donc d'écrire le terme  $(\mathbf{u} \cdot \nabla)\mathbf{u}$  sous cette forme et de considérer que l'équation est vérifiée au sens des distributions sur  $\Omega$ .

– La turbulence selon Leray. Le mouvement devient turbulent au moment où la solution régulière laisse place à une solution faible qui peut avoir du tourbillon (vorticité)  $\omega = \text{rot } \mathbf{u}$  infini en certains points.

– La question « la solution cesse-t-elle vraiment d'être régulière au bout d'un temps fini ? » est l'objet du prix Clay.

On voit que ce théorème règle en fait la situation des écoulements laminaires, mais le cas turbulent (qui correspond à  $\mathbf{u}_0$  ou  $T^*$  grand) lui échappe complètement car la seule existence sans unicité d'une solution faible est physiquement inconsistante.

### Et l'équation d'Euler ?

Le premier résultat important faisant le pendant avec celui de Leray remonte à Kato (1972).

**Théorème.** *Si  $\mathbf{u}_0$  est assez régulière, avec  $\text{div } \mathbf{u}_0 = 0$  et  $\mathbf{u}_0 \cdot \mathbf{n} = 0$  sur  $\partial\Omega$ , il existe un temps  $T^* > 0$  et une solution classique unique de (E) sur l'intervalle de temps  $[0, T^*]$ .*

Commentaires

- Ici, la régularité va s'exprimer par la vérification d'une condition de Hölder pour les dérivées de  $u_0$ .
- On ne sait rien sur l'existence d'éventuelles solutions faibles pour  $t > T^*$ .
- On vérifie aisément que, pour une solution régulière, l'énergie cinétique  $\frac{1}{2} \int_{\Omega} u^2 dx$  est conservée.

Si l'on veut maintenant résumer la situation, on peut dire qu'après pratiquement un siècle d'efforts acharnés on a mis en correspondance une énigme physique avec un problème mathématique extrêmement ardu. Il semblerait donc que, pour l'instant, on n'ait pas gagné grand chose.

Pour dépasser ce constat accablant, il nous faut maintenant être plus précis sur ce qu'attend le physicien.

**RETOUR A LA PHYSIQUE : QUE VEUT-ON EXPLIQUER ?**

On a vu dans ce qui précède que la situation turbulente correspond à  $Re$  grand.

**Le nombre de degrés de liberté**

Bien qu'en toute rigueur la description en terme de champ de vitesse d'un écoulement fluide implique un nombre de degrés de liberté infini, un raisonnement heuristique dû à Kolmogorov suggère qu'un écoulement visqueux ne dépend en fait que d'un nombre fini de degrés de liberté, de l'ordre de  $Re^{9/4}$ . Ce nombre représente la dimension de l'espace d'approximants qu'il faudrait prendre pour faire un calcul numérique raisonnable de la solution.

On voit que le nombre de degrés de liberté devient vite gigantesque dans un écoulement turbulent : pour le cas de la météorologie où nous avons estimé  $Re = 10^{12}$ , on obtient  $10^{27}$  ! C'est pourquoi la turbulence pose aujourd'hui, et posera encore demain, un sérieux problème de calcul numérique effectif.

Notons au passage que le raisonnement de Kolmogorov suppose que la solution de Navier-Stokes est suffisamment régulière pour qu'à petite échelle,  $u$  puisse être considéré comme sensiblement constant, ce qui est justement, pour le mathématicien, le fond du problème. En tout état de cause, nous retiendrons que l'état turbulent correspond à un très grand nombre de degrés de liberté.

Venons-en maintenant à ce que le physicien observe dans les écoulements turbulents. Pour cela, nous allons considérer deux cas bien distincts, suivant que l'écoulement s'effectue en dimension deux ou trois. Cette distinction n'a rien d'académique, c'est le reflet des phénomènes observés. L'approximation bidimensionnelle

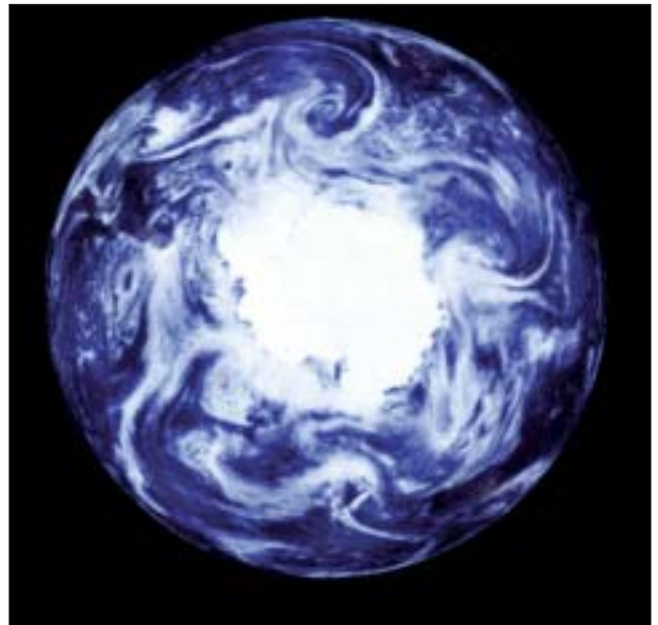


Figure 1 - Sur cette photographie satellite, on observe un système de quelques grands tourbillons atmosphériques, alternance d'anticyclones et de dépressions, entourant le pôle sud. Ces formations sont des « structures cohérentes » créées par l'auto-organisation caractéristique des écoulements turbulents bidimensionnels (photo NASA, mission Galileo).

(l'écoulement a lieu dans un plan ou sur une surface) est souvent utilisée en pratique lorsque le fluide est confiné dans une couche de faible épaisseur. Ainsi, lorsque l'épaisseur des couches fluides est négligeable par rapport aux échelles horizontales considérées, les mouvements de l'atmosphère ou des océans peuvent être considérés comme bidimensionnels.

Les traits principaux de la turbulence à deux dimensions sont la conservation de l'énergie cinétique et la tendance à former de grands tourbillons organisés stables (on les nomme structures cohérentes ; figure 1).

Par contraste, en dimension 3 (écoulement dans une soufflerie par exemple), il y a une forte dissipation d'énergie cinétique et on n'observe généralement pas de structures organisées. Les observations quantitatives reproductibles concernent le spectre d'énergie cinétique et la répartition statistique des incréments de vitesse  $u(t, x) - u(t, x')$  pour des points voisins  $x$  et  $x'$ .

Onsager fut le premier à distinguer aussi clairement les phénomènes à expliquer.

**LA TURBULENCE EN DIMENSION 2**

Suivant Onsager, il faut expliquer la conservation de l'énergie cinétique et l'apparition de structures organisées. Pour Onsager, l'équation d'Euler est parfaitement adaptée, car elle conserve l'énergie, et l'apparition générale de ces structures doit s'expliquer par une mécanique statistique de l'équilibre.

Un petit retour aux équations d'Euler et Navier-Stokes va nous éclairer.

En dimension 2 il se passe quelque chose de tout à fait remarquable : les avatars du théorème de Leray disparaissent :

- Pour  $\mathbf{u}_0$  régulière, la solution régulière de N-S existe pour tout temps.
- Pour  $\mathbf{u}_0$  peu régulière, la solution faible est unique.

De même pour l'équation d'Euler, la situation devient satisfaisante. En effet, en prenant le rotationnel de l'équation (E), on obtient l'équation en  $\omega = \text{rot } \mathbf{u}$  (la vorticit    $\omega$  est maintenant une fonction scalaire) :

$$(E_\omega) \quad \begin{cases} \frac{\partial \omega}{\partial t} + \text{div}(\omega \mathbf{u}) = 0, \\ \text{rot } \mathbf{u} = \omega, \text{div } \mathbf{u} = 0, \mathbf{u} \cdot \mathbf{n} = 0 \text{ sur } \partial\Omega. \end{cases}$$

C'est une   quation de transport (de  $\omega$  par  $\mathbf{u}$ ) coupl  e avec un syst  me elliptique ( $\mathbf{u}$  fonction de  $\omega$ ). On en d  duit le r  sultat d'existence et d'unicit   suivant :

**Th  or  me (Youdovitch 1963).** *Pour toute fonction mesurable born  e  $\omega_0$ , il existe une solution faible mesurable et born  e  $\omega(t, x)$  au probl  me  $(E_\omega)$ , admettant  $\omega_0$  comme condition initiale. Cette solution est unique.*

*Remarque*

La situation se complique consid  rablement si l'on s'autorise    prendre pour  $\omega_0$  une mesure, par exemple si le champ de vitesse initial est discontinu ; ce probl  me (dit des feuilles de tourbillon) n'est pas d  nu   de sens physique. Mais ici, une vorticit   initiale born  e suffira    notre propos.

Autre fait rassurant en dimension 2 : sous des conditions raisonnables, lorsque la viscosit   tend vers z  ro, la solution de Navier-Stokes correspondant    la donn  e initiale  $\mathbf{u}_0$  tend vers la solution de l'  quation d'Euler de m  me donn  e initiale. Par conditions raisonnables, on entend soit que l'on est dans le cas de solutions spatialement p  riodiques (  coulements sur le tore), soit que l'on remplace la condition de Stokes  $\mathbf{u} = 0$  au bord du domaine par une condition de friction sur le bord (qui est en fait celle qui avait   t   primitivement propos  e par Navier) qui, dans bien des cas, est physiquement plus r  aliste.

On d  duit des consid  rations ci-dessus qu'il est tout    fait l  gitime d'  tudier la turbulence 2D en prenant pour mod  le l'  quation d'Euler, qui donne bien le comportement des fluides dans la limite des faibles viscosit  s.

C'est ce qu'avait bien pressenti Onsager. Comme on peut montrer que la solution donn  e par le th  or  me de

Youdovitch conserve l'  nergie, la premi  re propri  t   de la turbulence 2D est clairement expliqu  e.

La formation des structures organis  es est une question plus complexe. Que se passe-t-il donc pour la solution de l'  quation d'Euler ? Gr  ce    la simulation num  rique, ce qui se passe est bien connu et peut   tre d  crit de mani  re imag  e en prenant pour  $\omega_0$  une tache de tourbillon ( $\omega_0$  vaut une valeur constante sur une certaine r  gion et 0 en dehors). Comme la vorticit    $\omega$  est simplement transport  e par un champ de vitesse incompressible,  $\omega$  va demeurer une tache de m  me surface    chaque instant mais cette tache va, en g  n  ral, se d  former de mani  re extr  mement complexe en   mettant des filaments de plus en plus fins au fur et    mesure qu'ils se d  forment et s'enroulent ; autrement dit,  $\omega$  se met    osciller    des   chelles spatiales de plus en plus petites. Si l'on se contente d'observer ainsi le flot de mani  re d  taill  e    petite   chelle,  $\omega$  devient de plus en plus compliqu  e et ne converge vers rien du tout ; c'est pourquoi on parle de chaos turbulent    petite   chelle. Si maintenant on cesse d'observer les d  tails et on fait une moyenne locale de  $\omega$     une certaine   chelle interm  diaire fix  e, on peut constater que cette moyenne converge ; autrement dit, pour  $t$  tendant vers l'infini,  $\omega(t, x)$  va converger pour la topologie faible vers une certaine fonction  $\omega^*$  (voir figure 2). Comme le rel  vement ( $\omega \rightarrow \mathbf{u}$ ) est compact, il s'ensuit que  $\mathbf{u}$  converge pour la norme  $L^2$  vers le champ de vitesse correspondant  $\mathbf{u}^*$ . Cet  $\mathbf{u}^*$  est le champ de vitesse qui d  crit la structure organis  e.

Comment montrer « qu'en g  n  ral » les choses se passent ainsi pour la solution des   quations d'Euler ? On ne sait pas le faire pour l'instant. En revanche, pour un  $\omega_0$  donn  , on sait trouver le bon candidat pour la limite  $\omega^*$ .

*D  termination de  $\omega^*$*

Pour ce faire, on met en   uvre le programme d'Onsager qui revient      tendre    l'  quation d'Euler la m  canique statistique de Boltzmann. La premi  re   tape consiste, au moyen de la th  orie des grandes d  viations,    construire la fonctionnelle entropie qui mesure pr  cis  ment la notion intuitive de d  sordre associ  e    un   coulement turbulent. La seconde est de r  soudre le probl  me variationnel consistant    maximiser cette entropie sous les contraintes associ  es    tous les invariants de l'  quation d'Euler. Le tout donne  $\omega^*$ .

Reste    d  montrer que  $\omega$  converge bien vers  $\omega^*$ , et on ne sait pas le faire. Comme tout r  sultat fourni par la m  canique statistique, il faudrait pour le justifier d  montrer, en un sens appropri  , l'ergodicit   du syst  me dynamique d  fini par l'  quation d'Euler 2D (syst  me hamiltonien de dimension infinie). On peut en revanche v  rifier par des simulations num  riques et des exp  riences en laboratoire que le comportement est correctement d  crit.

**LA TURBULENCE EN DIMENSION 3**

En dimension trois, on dispose d'observations et de mesures faites en soufflerie ; le tout est résumé depuis de nombreuses décennies sous la forme de quelques grandes lois expérimentales.

Notons tout d'abord que l'on n'observe généralement pas la formation de structures comme en dimension deux.

La première loi concerne la dissipation d'énergie ; elle est formulée d'une manière assez étonnante car elle fait appel à une opération par la pensée.

**Loi de la dissipation d'énergie**

Dans une expérience de turbulence, tout le reste étant fixé, si la viscosité tend vers zero la dissipation d'énergie cinétique par unité de masse tend vers une limite non nulle :

$$\frac{dE}{dt} \longrightarrow D,$$

$D$ , qui a pour dimension  $L^2T^{-3}$ , est fonction de « l'intensité » de la turbulence.

$\frac{dE}{dt}$  désigne ici une quantité moyenne, prise sur tout le domaine.

Ainsi donc, la dissipation d'énergie dans un flot turbulent 3D ne dépend pas de la viscosité.

**Loi des 2/3**

Considérons une portion  $\Omega$  du domaine dans lequel s'effectue l'écoulement turbulent ; à chaque instant  $t$  fixé, et on a :

$$\frac{1}{|\Omega|} \int_{\Omega} |\mathbf{u}(t, x + \xi) - \mathbf{u}(t, x)|^2 dx \approx \text{cte} |\xi|^{2/3}.$$

La constante du second membre ne dépend pas de  $\Omega$  mais uniquement de  $D$ .

Cette deuxième loi donne une information importante sur la régularité du champ de vitesse turbulent.

A la première loi s'en associe naturellement une autre, qui n'est pas expérimentale et jouit d'un statut particulier, car c'est la seule loi sur la turbulence que l'on sache « démontrer » (au sens physique du terme) à partir de la dynamique du système (équation de Navier-Stokes).

**La loi du 4/5**

Elle est issue des calculs de Von Karmàn et Howarth en 1938, complétés par Kolmogorov en 1941. Une ver-

sion plus générale (sans hypothèse d'isotropie) très intéressante en a été donnée par Monin en 1959.

Pour énoncer cette loi, on suppose que le champ de vitesse turbulent est représenté par une solution aléatoire des équations de Navier-Stokes  $\mathbf{u}(t, x, a)$  ( $a$  désignant le paramètre aléatoire), c'est-à-dire que pour tout  $a$  fixé  $\mathbf{u}(t, x, a)$  est une solution des équations de Navier-Stokes (en un sens qui ne peut être que faible car, d'après la loi des 2/3, le champ ne peut pas être bien régulier). On fait quelques hypothèses sur ce champ aléatoire.

(i) Il est de moyenne nulle : pour tous  $t, x$  on a  $\langle \mathbf{u}(t, x, a) \rangle = 0$ ,  $\langle \rangle$  désignant la moyenne d'ensemble.

(ii) Il est homogène en espace : pour tous  $t, \xi$ , le champ aléatoire  $\mathbf{u}(t, x + \xi, a)$  a la même loi que  $\mathbf{u}(t, x, a)$ .

(iii) Il est isotrope au sens fort : pour toute matrice réelle unitaire  $A$ , le champ aléatoire  ${}^t A \mathbf{u}(t, Ax, a)$  a la même loi que  $\mathbf{u}(t, x, a)$ .

On note  $\delta \mathbf{u} = \mathbf{u}(t, x + \xi, a) - \mathbf{u}(t, x, a)$ , et la loi du 4/5 s'énonce alors :

$$(4/5) \quad \left\langle \left( \delta \mathbf{u} \cdot \frac{\xi}{|\xi|} \right)^3 \right\rangle = -\frac{4}{5} D |\xi|.$$

**Commentaires**

1.  $D$  est la constante qui intervient dans la loi de dissipation ; la formule ci-dessus relie donc de manière étonnamment simple la dissipation d'énergie du flot turbulent à la statistique des incréments de vitesse.

2. On n'a pas fait d'hypothèse de stationnarité sur le champ  $\mathbf{u}$ , ni d'hypothèse d'invariance par changement d'échelle.

3. Il existe une version non isotrope de ce résultat (Monin) qui s'exprime :

$$D = -\frac{1}{4} \text{div}_{\xi} \langle (\delta \mathbf{u})^2 \delta \mathbf{u} \rangle_{\xi=0}.$$

4. La formule (4/5) s'obtient par des manipulations formelles à partir de l'équation de Navier-Stokes, puis en prenant la limite ( $\nu \rightarrow 0$ ). La justification mathématique de la méthode paraît inaccessible avec des hypothèses raisonnables sur le champ de vitesse (j'entends par là des hypothèses que l'on sait expérimentalement vérifiées par le champ turbulent et pas plus). Cette loi n'en est pas moins considérée comme parfaitement valide par les physiciens de la turbulence (cf. Frisch).

Une théorie convenable de la turbulence doit retrouver rigoureusement ces lois à partir des équations du mouvement fluide (Navier-Stokes ou Euler). Mais le choix du

modèle de base pour le faire nous plonge d'entrée dans la perplexité.

### Visqueux ou pas visqueux ?

On a montré au paragraphe précédent qu'en dimension 2, la clarification mathématique du problème permettait d'étudier la turbulence à partir de l'équation d'Euler, ce qui simplifiait considérablement les choses. Qu'en est-il en dimension 3 ? Comme on l'a vu, les résultats connus jusqu'à ce jour ne sont pas d'un grand secours.

Le fait que la dissipation d'énergie soit importante a conduit une grande majorité de physiciens à penser que la viscosité, même évanescence, continue à jouer un rôle. Il faut donc étudier l'équation de Navier-Stokes, quitte ensuite à opérer un passage à la limite ( $\nu \rightarrow 0$ ). C'était aussi le point de vue de Leray. En effet, celui-ci se méfiait de l'équation d'Euler à cause du paradoxe de d'Alembert<sup>1</sup>, paradoxe que l'on peut effectivement présenter comme la partie la plus visible d'un iceberg d'avatars contenus dans cette équation, comme par exemple la non-unicité au problème de Cauchy, mais c'est une autre histoire...

Je vais maintenant présenter une autre façon de voir les choses, qui a été quelque peu oubliée : elle est due à Onsager<sup>2</sup>.

Pour Onsager, il saute aux yeux dans la loi du 4/5 que la viscosité n'intervient pas ; la dissipation apparaît simplement reliée à la non-régularité du champ de vitesse. Il faut supposer que  $\nu = 0$  et donc travailler avec l'équation d'Euler. Le problème est alors que l'équation d'Euler est un système hamiltonien, censé conserver l'énergie. Mais examinons comment on montre la conservation de l'énergie pour une solution de l'équation d'Euler (plaçons-nous dans le cadre de solutions spatialement périodiques pour simplifier).

On part de l'équation  $\frac{\partial \mathbf{u}}{\partial t} + (\mathbf{u} \cdot \nabla) \mathbf{u} = -\nabla p$  ; on la multiplie scalairement par  $\mathbf{u}$  et on intègre sur le tore, d'où

$$\int \frac{\partial \mathbf{u}}{\partial t} \cdot \mathbf{u} dx + \int u_i \partial_i u_k u_k dx = - \int \nabla p \cdot \mathbf{u} dx,$$

où l'on utilise la convention usuelle sur la sommation des indices.

<sup>1</sup> Sous sa forme la plus aboutie, ce paradoxe énonce que pour un écoulement de fluide parfait stationnaire, irrotationnel et constant à l'infini, autour d'un obstacle borné de l'espace, la résultante des forces de pression exercées sur l'obstacle est nulle.

<sup>2</sup> Lars Onsager a reçu le prix Nobel de chimie en 1968 pour la découverte des relations de réciprocité en thermodynamique linéaire.

On note que  $u_i \partial_i u_k u_k = u_i \partial_i \left( \frac{1}{2} \mathbf{u}^2 \right)$  et on voit maintenant, en effectuant une intégration par parties, que les deux dernières intégrales sont nulles car  $\text{div } \mathbf{u} = 0$ . Il ne reste plus qu'à remarquer que la première intégrale est égale à la dérivée par rapport au temps de l'énergie cinétique.

Pour justifier ce calcul, il faut au minimum que toutes les expressions écrites aient un sens, ce qui suppose une certaine régularité du champ  $\mathbf{u}$ . Onsager imagine alors que la turbulence est modélisée par des solutions (en un sens généralisé) de l'équation d'Euler, suffisamment peu régulières pour que l'énergie ne soit pas conservée. Les solutions imaginées par Onsager sont exactement les solutions faibles que nous avons précédemment définies.

De telles solutions existent-elles ? Oui, Shnirelman a construit récemment un exemple de solution faible qui dissipe l'énergie cinétique.

On a donc des candidats potentiels pour représenter le flot turbulent : ce sont des solutions faibles des équations d'Euler qui dissipent l'énergie. Malheureusement, on n'a pas de résultat général d'existence pour de telles solutions (on ne sait pas résoudre le problème de Cauchy avec une donnée initiale peu régulière) et encore moins de résultat d'unicité.

On peut tout de même faire un petit pas de plus dans cette direction.

On peut tout de même faire un petit pas de plus dans cette direction.

### Conjecture d'Onsager et bilan local d'énergie pour des solutions faibles

En s'appuyant sur la loi du 4/5, Onsager avait conjecturé (en 1949) que les solutions faibles d'Euler qui vérifient une condition de Hölder d'ordre strictement plus grand que 1/3 doivent conserver l'énergie.

Cette conjecture est restée dans l'oubli jusqu'en 1992 quand Eyink a rappelé l'intérêt de ce problème et fourni une preuve d'un énoncé plus faible. En 1994, les trois mathématiciens Constantin, E (c'est son nom !) et Titi ont donné une preuve esthétique et simple d'un énoncé plus fort.

Mais on peut faire mieux et expliciter précisément ce qu'est la dissipation locale d'énergie par défaut de régularité.

**Théorème (Duchon et Robert 2000).** *Soit  $\mathbf{u}$  une solution faible de l'équation d'Euler sur le tore  $\Pi^3$ , telle que  $|\mathbf{u}|^3$  soit intégrable sur  $]0, T[ \times \Pi^3$ . Soit  $\varphi$  une fonction indéfiniment dérivable à support compact sur  $\mathbb{R}^3$ , positive, d'intégrale égale à 1 et symétrique. Pour  $\varepsilon > 0$ , notons*

$$\varphi^\varepsilon(\xi) = \frac{1}{\varepsilon^3} \varphi\left(\frac{\xi}{\varepsilon}\right),$$

et 
$$D_\varepsilon(\mathbf{u}) = \frac{1}{4} \int \nabla \varphi^\varepsilon(\xi) \cdot \delta \mathbf{u} (\delta \mathbf{u})^2 d\xi$$

Alors, lorsque  $\varepsilon$  tend vers 0,  $D_\varepsilon(\mathbf{u})$  (qui est une fonction de  $t$  et  $x$ ) converge, au sens des distributions sur  $]0, T[ \times \Pi^3$ , vers une distribution  $D(\mathbf{u})$ , indépendante de  $\varphi$ , et on a le bilan local d'énergie :

$$\partial_t \left( \frac{1}{2} \mathbf{u}^2 \right) + \operatorname{div} \left( \left( \frac{1}{2} \mathbf{u}^2 + p \right) \mathbf{u} \right) + D(\mathbf{u}) = 0.$$

**Commentaires**

1. La démonstration découle de quelques manipulations simples à partir d'une version régularisée de l'équation d'Euler.
2. A partir de ce résultat, en intégrant l'équation du bilan local sur tout le domaine, on déduit immédiatement une preuve de la conjecture d'Onsager sous l'hypothèse de régularité sur le champ de vitesse :

$$\int |\mathbf{u}(t, x + \xi) - \mathbf{u}(t, x)|^3 dx \leq c(t) |\xi| \sigma(|\xi|),$$

où  $\sigma(r)$  tend vers 0 lorsque  $r$  tend vers 0 et  $\int_0^T c(t) dt < \infty$ .

3. L'équation du bilan local d'énergie amène à imposer une condition naturelle aux éventuelles solutions faibles censées représenter le flot turbulent : l'énergie ne peut qu'être dissipée et non pas créée au sein du fluide ; on supposera donc que  $D(\mathbf{u})$  est une distribution positive (donc une mesure).

Cette condition est bien sûr à rapprocher des conditions d'entropie qui interviennent dans l'étude des équations hyperboliques non linéaires. Nous y reviendrons au paragraphe suivant.

4. Il est aisé à partir de cette formule d'établir une preuve rigoureuse de la loi du 4/5 sous des hypothèses raisonnablement faibles sur le champ de vitesse aléatoire.

**UN MODÈLE INSTRUCTIF : L'ÉQUATION DE BURGERS A UNE DIMENSION**

Le sens de la condition ( $D(\mathbf{u}) \geq 0$ ), que nous avons imposée de manière abrupte, peut être éclairé par un détour du côté de l'équation de Burgers.

Commençons par rappeler quelques faits bien connus en ce qui concerne les équations hyperboliques non linéaires en général (penser par exemple aux équations régissant l'évolution d'un gaz compressible non visqueux). Pour ces équations, on est également obligé de

travailler avec des solutions faibles non régulières. La raison en est que, partant d'une donnée initiale régulière, la solution a tendance à former des chocs au bout d'un temps fini, c'est-à-dire que des discontinuités apparaissent. Ce phénomène est très général et peut être explicitement décrit sur l'équation la plus simple de ce type, à savoir l'équation de Burgers en dimension un d'espace :

$$(B) \quad \partial_t u + \partial_x \left( \frac{1}{2} u^2 \right) = 0,$$

où  $u$  est maintenant une fonction scalaire définie sur la droite réelle.

Pour cette équation, on montre facilement qu'en partant d'une donnée initiale régulière (par exemple  $u_0$  indéfiniment dérivable à support compact) il existe une unique solution régulière sur un intervalle fini  $[0, T^*[$ , en  $T^*$  des discontinuités apparaissent dans la solution. Si  $u_0$  est seulement supposée intégrable, on peut montrer qu'il existe pour tout temps une solution faible. Le problème avec les solutions faibles est que l'on perd l'unicité pour le problème de Cauchy : on peut avoir plusieurs solutions correspondant à la même donnée initiale. Il faut alors rajouter une condition pour sélectionner la « bonne » solution : la condition d'entropie de Lax. Dans le cas de l'équation de Burgers, cette condition revient à dire que les discontinuités de la solution sont à sauts négatifs. La justification que cette condition sélectionne la solution physiquement admissible est liée au fait que l'information contenue dans la donnée initiale ne peut qu'être détruite et non pas créée au niveau des chocs ; on peut aussi montrer que cette solution est limite de la solution visqueuse obtenue en rajoutant une petite viscosité dans le système et en faisant tendre cette viscosité vers zéro. On peut alors montrer qu'il existe une seule solution faible entropique au problème de Cauchy (théorème de Kruzhkov).

Le calcul sur le bilan local d'énergie pour les solutions faibles de l'équation d'Euler s'étend aux solutions faibles de l'équation de Burgers ; il donne :

$$\partial_t \left( \frac{1}{2} u^2 \right) + \partial_x \left( \frac{1}{3} u^3 \right) + D(u) = 0.$$

Si l'on suppose que  $u$  est discontinue aux points  $x_i$  avec des limites à droite et à gauche  $u_i^+$  et  $u_i^-$ , on peut expliciter la distribution  $D(u)$  :

$$D(u) = -\frac{1}{12} \sum_i (u_i^+ - u_i^-)^3 \delta_{x_i},$$

la condition d'entropie de Lax s'écrit donc ici aussi  $D(u)$  positif, et on voit bien que la dissipation d'énergie a lieu au niveau des chocs.

## Solutions statistiques

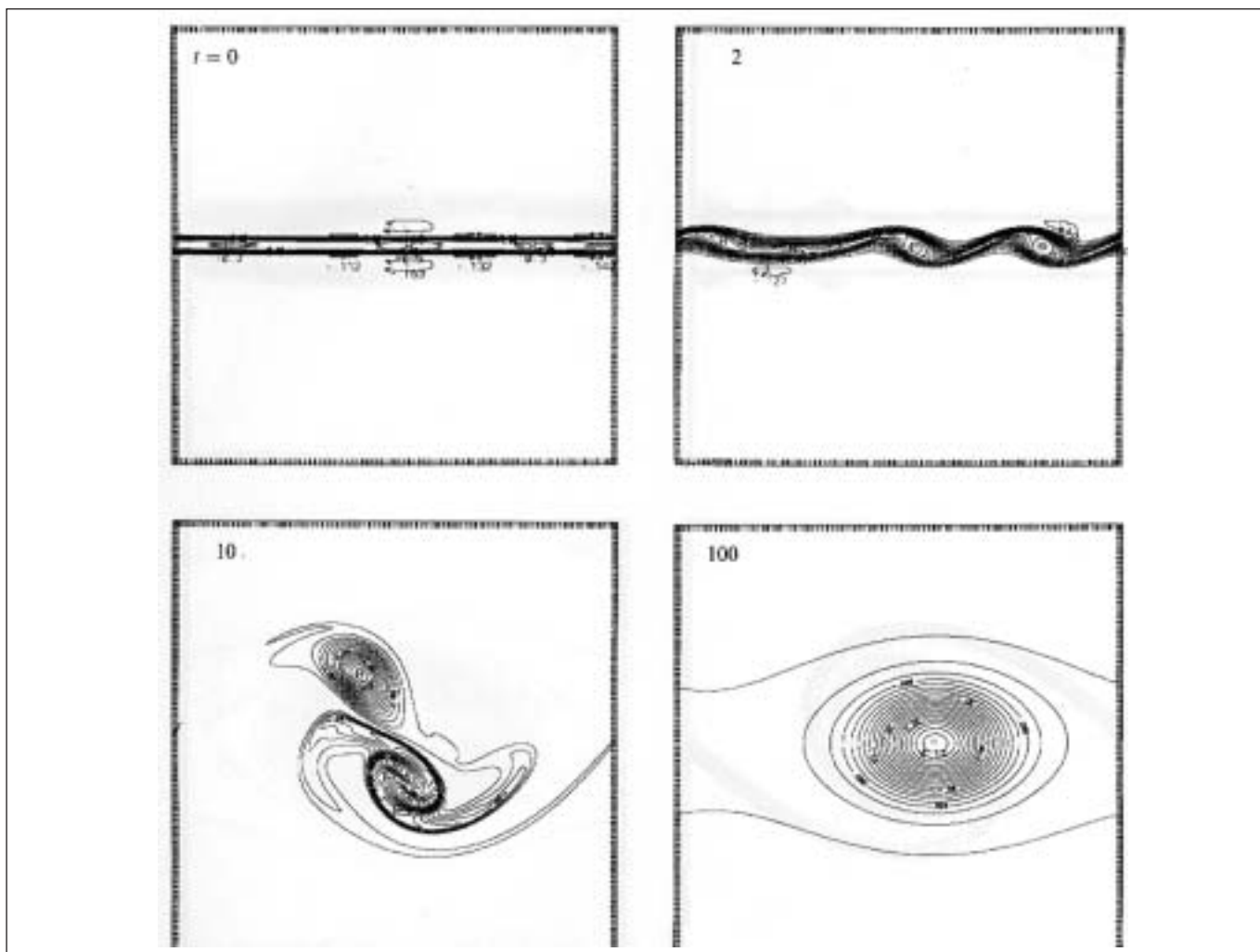
On a vu que dans un écoulement turbulent, le nombre de degrés de liberté était gigantesque ; il s'ensuit que les observations physiques reproductibles ont un caractère statistique (que ce soit la formation des structures cohérentes ou les lois sur la dissipation d'énergie et la distribution des incréments de vitesse). D'un point de vue mathématique, cela pose le problème de la recherche de solutions statistiques. *A priori* le concept de solution statistique d'une équation d'évolution est simple ; on suppose que la donnée initiale est une fonction ou un champ de vecteur qui dépend d'un paramètre aléatoire et on lui associe la solution à l'instant  $t$  qui est donc une fonction aléatoire. Cette façon de voir est claire si l'on dispose d'un bon semi-groupe résolvant le problème de Cauchy ; comme ce n'est pas toujours le cas, on a généralement recours à des définitions plus larges de la notion de solution statistique, définitions qui vont poser des problèmes

épineux (comme l'unicité) mais dont l'intérêt est de pouvoir tout de même chercher des solutions statistiques d'équations pour lesquelles on ne sait pas résoudre le problème de Cauchy (Euler par exemple). Même dans les bons cas, où l'on dispose d'un semi-groupe, le fond du problème est de décrire le champ aléatoire à l'instant  $t$  en fonction de l'état initial.

Explicitons la démarche sur l'exemple modèle de l'équation de Burgers.

On va prendre comme condition initiale  $u_0$  un processus en  $x$  :  $u_0(x, a)$  ( $a$  paramètre aléatoire). Le flot de l'équation de Burgers (ou, si l'on préfère, le semi-groupe donnant la solution entropique unique) va donner à l'instant  $t$  un nouveau processus  $u(t, x, a)$ . Que peut-on en dire ?

La première avancée sur cette question est due à Sinai (en 1992) : il prend pour  $u_0$  le mouvement brownien issu de 0. Il arrive alors à décrire à l'instant  $t$  le processus



**Figure 2** - Simulation numérique de l'évolution d'un fluide plan dont l'état initial est constitué d'une bande mince où la vorticité a une valeur constante (et nulle en dehors). La bande est instable et des tourbillons se forment. Les courbes représentent ici les lignes d'isovorticité. Finalement un état stationnaire, constitué d'un tourbillon unique, est atteint. La petite viscosité indispensable pour assurer la stabilité du calcul a pour effet de lisser les oscillations de la vorticité en dessous d'une certaine échelle spatiale ; c'est pourquoi on observe la convergence vers un état stationnaire. Ce phénomène est très général (simulations dues à J. Sommeria, C. Staquet et R. Robert, effectuées sur le CRAY 2 du CCVR).

$u(t, x, a)$  : c'est un processus de Lévy, processus bien connu qui peut avoir des sauts. Pour ce faire, Sinai utilise la construction classique de Hopf-Cole qui permet d'expliciter la solution faible entropique de l'équation de Burgers en fonction de la donnée initiale.

La deuxième avancée est celle de Carraro et Duchon (en 1994) : ces auteurs considèrent le cas où  $u_0$  est un processus de Lévy homogène sur la droite (c'est-à-dire invariant par translation) et à sauts négatifs. Ils montrent qu'à l'instant  $t$   $u(t, x, a)$  est encore un processus de Lévy homogène à sauts négatifs ; de plus, ils obtiennent explicitement l'équation d'évolution régissant l'évolution de l'exposant de Lévy du processus (un processus de Lévy homogène est commodément décrit au moyen d'une certaine fonction que l'on appelle son exposant de Lévy).

La troisième avancée est due à Bertoin (1998) : Bertoin traite le cas d'un  $u_0$  processus de Lévy issu de 0. Contrairement aux auteurs précédents, Bertoin utilise comme Sinai la transformation de Hopf-Cole alors que Carraro et Duchon s'en passent et sont amenés à introduire la notion de solution statistique intrinsèque (notion particulièrement intéressante, car elle donne une réponse naturelle au problème de la divergence infrarouge, omniprésent en turbulence).

La quatrième avancée est due à Chabanol et Duchon (2002) : ils prennent cette fois pour  $u_0$  un processus de Markov homogène sur la droite, à sauts négatifs ; à tout instant  $u$  reste un processus de Markov homogène à sauts négatifs. Ils obtiennent en outre l'équation d'évolution portant sur le noyau de transition du processus.

Bien sûr, je ne prétends pas être exhaustif au sujet de l'équation de Burgers et j'écarte à regret bien d'autres contributions fort intéressantes. Cette histoire n'est évidemment pas finie et bien des questions demeurent, comme le rôle de l'homogénéité ou la question de l'unicité des solutions statistiques, plus la grande question de savoir comment obtenir ce type de résultat pour d'autres équations, celle d'Euler par exemple.

### CONCLUSION

Quels sont les bons objets décrivant le flot turbulent ? Peut-être des solutions faibles des équations d'Euler, comme l'annonçait Onsager ; en tout cas, rien pour l'instant ne l'interdit. Alors, la description des propriétés statistiques du flot turbulent doit s'obtenir à partir d'une solution statistique convenablement définie.

Il se pourrait également que la bonne équation limite ne soit pas celle d'Euler mais un modèle plus complexe faisant intervenir les oscillations locales du champ de vitesse.

En tout état de cause, la clé du problème semble davantage contenue dans les équations d'Euler que dans Navier-Stokes. En effet, quand bien même on saurait résoudre convenablement le problème de Cauchy pour les équations de Navier-Stokes, il faut faire tendre la viscosité vers zéro pour comprendre la turbulence à trois dimensions. Il y a peu de chance que l'on sache dire quelque chose sur cette limite, sans information sur le comportement d'une équation limite (celle d'Euler ?).

### POUR EN SAVOIR PLUS

Sur l'œuvre de Jean Leray, voir l'article de **Jean-Yves Chemin** dans la *Gazette des mathématiciens*, supplément au numéro 84 (2000).

Sur les équations hyperboliques non linéaires et la condition d'entropie, voir le livre de **Denis Serre**, *Systèmes de lois de conservation I*. Diderot éditeur, 1996.

Sur la turbulence sous l'angle du physicien, voir le livre d'**Uriel Frisch**, *Turbulence*. Cambridge University Press, 1995.

Voir aussi l'article de **Lars Onsager**, *Statistical hydrodynamics*. Nuovo Cimento, 6 (2), 279-287, 1949.

Sur les résultats évoqués ici et certaines de leurs conséquences, voir mon article à paraître, *Statistical hydrodynamics. Handbook of mathematical fluid mechanics*, vol. 2, Friedlander and Serre editors, 2003.

Sur l'équation de Burgers et les processus de Lévy, voir l'article de **Carraro et Duchon**, Ann. Inst. Henri Poincaré, *Analyse non linéaire*, vol. 15, 4, p. 431-458, 1998 et celui de **Bertoin**, *Comm. Math. Phys.*, 193, 397-406, 1998.



# A la recherche de mots de fréquence exceptionnelle dans les génomes

**La compréhension de l'information génétique portée par les génomes est un défi pour les biologistes, les biophysiciens, les informaticiens et les mathématiciens. L'un des problèmes classiques en bioinformatique est l'identification de « mots » qui apparaissent avec une fréquence inattendue dans ces longues suites de lettres à valeur dans l'alphabet  $\{a, c, g, t\}$  que sont les séquences d'ADN. Ces mots exceptionnels peuvent en effet être liés à des mécanismes biologiques cruciaux pour la cellule. Nous présentons ici la démarche du statisticien face à cet enjeu.**

L'information génétique de chaque être vivant est portée par son ADN. Celui-ci est une longue succession de nucléotides. Il existe quatre nucléotides différents selon qu'ils portent l'une des bases *adénine*, *cytosine*, *guanine* ou *thymine*. Ainsi, une manière d'appréhender l'ADN est de le considérer comme un texte écrit sur un alphabet à quatre lettres  $\{a, c, g, t\}$ . Nous allons nous intéresser ici aux mots – courtes suites de nucléotides – contenus dans une séquence d'ADN donnée, et plus particulièrement à leur fréquence d'apparition.

## MOTS EXCEPTIONNELS

Chaque occurrence d'un mot peut être reconnue par une enzyme et ainsi participer à un mécanisme biologique. C'est le cas par exemple des sites de restriction chez les bactéries, généralement constitués de 6 nucléotides (ou lettres), qui constituent des points de cassure de l'ADN dès qu'ils sont reconnus par une enzyme de restriction spécifique. Il n'est donc pas surprenant que ces sites soient spécialement évités dans les génomes bactériens car ils fragilisent l'ADN. A l'inverse, certains mots sont primordiaux pour garantir une certaine stabilité du génome et sont donc présents en grand nombre le long de l'ADN. C'est le cas du mot *gctggtgg* qui est très fréquent dans le génome de la bactérie *E. coli*. On y reviendra à la fin de ce texte. Rechercher des mots significativement rares ou fréquents ou détecter si un mot donné est exceptionnel dans une séquence est donc devenu un problème classique en génomique. Voyons comment poser le problème de façon statistique.

## PROBLÈME STATISTIQUE

On souhaite savoir si un mot  $W$  donné, sur l'alphabet  $\mathcal{A} = \{a, c, g, t\}$ , a une fréquence d'apparition inattendue dans une séquence d'ADN donnée de longueur  $n$ , c'est-à-dire soit trop forte, soit trop faible. Pour cela, il faut définir ce qu'est une valeur attendue ou espérée du nombre d'occurrences du mot  $W$  dans une séquence de longueur  $n$  et la variabilité autour de cette valeur. De façon plus précise, il faut déterminer la loi probabiliste du comptage ; cela nécessite de définir un modèle. Un modèle est, d'une part, l'ensemble de toutes les séquences possibles dont la séquence d'ADN observée n'est qu'une réalisation et, d'autre part, une loi de probabilité sur cet ensemble. On verra que le modèle choisi a une influence sur le caractère exceptionnel d'un mot. La significativité de la fréquence observée n'a en effet de sens que par rapport à une fréquence attendue, celle déterminée par le modèle. En changeant de modèle, on modifie la fréquence attendue et l'écart entre la fréquence observée et celle attendue peut devenir significatif ou, au contraire, ne plus l'être. Si on fait l'analogie avec un texte en français, la combinaison de lettres « tra » est beaucoup plus fréquente que « tsa » car « tr » est déjà plus fréquente que « ts ». De même, il est tout à fait possible que sur un génome *tgg* soit beaucoup plus fréquent que *tcg* car *tg* serait plus fréquent que *tc*. Lorsque l'on souhaite étudier de courtes séquences d'ADN comme des mots, il est donc probablement pertinent d'utiliser des modèles qui prennent en compte la fréquence des sous-mots qui les composent. On verra qu'une des réponses consiste à utiliser des modèles de chaînes de Markov.

---

– Sophie Schbath, INRA, Unité mathématique, informatique & génome, 78352 Jouy-en-Josas.  
tél. 01 34 65 28 90, [sophie.schbath@jouy.inra.fr](mailto:sophie.schbath@jouy.inra.fr)

Ont également participé à ce travail V. Brunaud, M. El Karoui, B. Prum, S. Robin, F. Rodolphe et E. de Turckheim.

Une fois le modèle choisi (chaîne de Markov d'ordre  $m$  par exemple), l'objectif est d'évaluer la probabilité  $\mathbb{P}(N(W) \geq c(W))$ , communément appelée  $p$ -valeur, où  $c(W)$  est le comptage observé du mot  $W$  dans la séquence d'ADN de longueur  $n$  et  $N(W)$  est la variable aléatoire qui représente le nombre d'occurrences de  $W$  dans une chaîne de Markov d'ordre  $m$  et de longueur  $n$ . En effet, si la  $p$ -valeur est très proche de 0 alors le mot  $W$  sera considéré comme exceptionnellement fréquent – ou significativement sur-représenté (il y a une probabilité quasi nulle de l'avoir observé autant de fois). Au contraire, si la  $p$ -valeur est très proche de 1, alors la probabilité  $\mathbb{P}(N(W) < c(W))$  est très proche de 0 et le mot est exceptionnellement rare – ou significativement sous-représenté (il y a une probabilité quasi nulle de l'avoir observé si peu de fois).

### ÉTAT DE L'ART

Plusieurs méthodes ont été développées pour évaluer cette  $p$ -valeur. L'une des plus récentes repose sur le calcul de la loi exacte du comptage  $N(W)$ , c'est-à-dire des probabilités  $\mathbb{P}(N(W) = x)$  pour tout entier  $x$ . Cette loi est déterminée par sa fonction génératrice et les probabilités ponctuelles peuvent s'obtenir par une récurrence. Cependant, cette méthode est pour le moment coûteuse en temps de calcul pour des longues séquences (et des mots fréquents) et n'est pas disponible en pratique pour des chaînes de Markov d'ordre  $m \geq 2$ , ce qui est limitant pour l'analyse des mots exceptionnels comme on le verra plus tard.

Auparavant, deux approximations de la loi du comptage ont été proposées pour des séquences suffisamment longues ( $n \rightarrow \infty$ ) : une approximation gaussienne valable pour des mots relativement fréquents (des mots pas trop longs par rapport à la longueur de la séquence) et une approximation par une loi de Poisson composée valable pour des mots rares (mots relativement longs par rapport à la longueur de la séquence). Sans rentrer dans les détails, on peut avoir une idée intuitive de ces deux résultats asymptotiques. On verra que le comptage  $N(W)$  du mot  $W$  n'est rien d'autre qu'une somme de variables aléatoires de Bernoulli  $Y_i$  non indépendantes, de même moyenne  $\mu(W)$ , qui valent 1 si le mot apparaît en position  $i$  dans la séquence ou 0 sinon. Si ces variables aléatoires étaient indépendantes, le comptage suivrait alors une loi binomiale  $\mathcal{B}(n, \mu(W))$  qui s'approche selon des résultats classiques soit par une loi normale si  $n\mu(W) \rightarrow \infty$ , soit par une loi de Poisson si  $n\mu(W)$  tend vers une constante quand  $n \rightarrow \infty$  (notons que  $n\mu(W)$  est précisément le comptage moyen). La difficulté réside ici dans le fait que les variables aléatoires  $Y_i$  ne sont pas indépendantes. Toutefois, il est démontré que l'on peut approcher la loi du comptage par une loi gaussienne ou par une loi de Poisson composée selon les

cas (quelques détails vont suivre) ; le prix à payer sera de tenir compte de la structure auto-recouvrante des mots (tttt est par exemple très recouvrant tandis que ttac ne l'est pas).

### MODÈLES POUR LES SÉQUENCES

Le choix du modèle correspond ici à définir une séquence  $S$  de  $n$  variables aléatoires  $X_1, X_2, \dots, X_n$ , à valeur dans l'alphabet  $\mathcal{A} = \{a, c, g, t\}$  qui « ressemblerait » en un certain sens à la séquence d'ADN donnée. Cela nous permettra de comparer ce qui est observé dans la séquence étudiée à ce à quoi l'on s'attendrait dans une séquence aléatoire générée selon le modèle. Rappelons ici que l'objectif n'est pas de modéliser au mieux une séquence d'ADN mais précisément de construire un modèle aléatoire qui prenne en compte certaines contraintes, certaines informations sur la séquence étudiée, pour détecter des écarts au modèle, c'est-à-dire des événements exceptionnels, compte tenu des contraintes déjà prises en compte.

#### Le modèle de Bernoulli

Un premier modèle consiste à supposer que les lettres  $X_i$  sont indépendantes les unes des autres et que les bases  $a, c, g$  et  $t$  apparaissent avec les probabilités  $\mu(a), \mu(c), \mu(g)$  et  $\mu(t)$  (la somme étant égale à 1). Notons M0 ce modèle. Dans le modèle M0, la vraisemblance, c'est-à-dire la probabilité de la suite  $S = X_1 X_2 \dots X_n$ , s'écrit

$$\prod_{b \in \mathcal{A}} (\mu(b))^{N(b)}$$

où  $N(b)$  est le nombre de  $b$  dans la séquence  $S$ . La statistique exhaustive du modèle M0 est donc le comptage de chacune des 4 bases. Choisir le modèle M0 consiste à ne retenir de la séquence que sa composition en bases  $a, c, g$  et  $t$ . Les paramètres  $\mu(b)$  étant inconnus dans notre cas, on les estime au vu d'une séquence observée par ceux qui maximisent la vraisemblance ci-dessus, c'est-à-

dire par les proportions :  $\hat{\mu}(b) = \frac{N(b)}{n}$ . Ainsi en

moyenne, le nombre de  $b$  dans les séquences aléatoires générées sous ce modèle M0 sera égal au nombre de  $b$  dans la séquence d'ADN.

#### Les chaînes de Markov

Un modèle qui permettrait de plus de prendre en compte la fréquence des 16 mots de longueur 2,  $aa, ac, \dots, tc$  et  $tt$ , est le modèle de chaîne de Markov stationnaire d'ordre 1, noté M1 dans la suite. En effet, notons  $\mu(\cdot)$  la mesure stationnaire sur  $\mathcal{A}$  et  $\pi(\cdot, \cdot)$  les probabilités de transition de la chaîne ; la vraisemblance s'écrit

alors

$$\mu(X_1) \prod_{a,b \in \mathcal{A}} \left( \pi(a, b) \right)^{N(ab)}$$

où  $N(ab)$  est le nombre de mots  $ab$  dans la séquence  $S$ . La statistique exhaustive du modèle M1 est composée de la première lettre  $X_1$  de la séquence et de la collection des comptages des 16 mots de longueur 2 sur l'alphabet  $\mathcal{A}$ . Les estimateurs du maximum de vraisemblance des paramètres sont  $\hat{\mu}(a) = \frac{N(a)}{n}$  et

$$\hat{\pi}(a, b) = \frac{N(ab)}{\sum_{b \in \mathcal{A}} N(ab)} \simeq \frac{N(ab)}{N(a)}$$

c'est-à-dire que la probabilité  $\pi(a, b)$  qu'un  $a$  soit suivi d'un  $b$  est estimée par la proportion de  $a$  suivis d'un  $b$ .

De la même façon, le modèle de chaîne de Markov stationnaire d'ordre  $m$ ,  $M_m$ , permettra de prendre en compte la composition de la séquence d'ADN en mots de longueurs 1 à  $(m + 1)$ . Un mot  $W$  de longueur  $h$  peut donc être étudié dans les modèles  $M_m$  avec  $0 \leq m \leq h - 2$ . Le modèle d'ordre  $m = h - 2$  est dit « maximal » pour étudier les mots de longueur  $h$ . C'est celui qui prend en compte la composition de la séquence d'ADN en mots de longueur  $h - 1$ .

Pour tenir compte d'une réalité biologique, à savoir que certaines séquences d'ADN (les gènes) codent pour des protéines et sont naturellement lues de 3 bases en 3 bases (les codons), il est souvent pertinent d'utiliser un modèle où par exemple la probabilité de transition de gtcg vers a (modèle M4) diffère selon que le a est la première, deuxième ou troisième base d'un codon. Les probabilités de transition sont alors périodiques de période 3, ce qui revient en fait à avoir 3 matrices de transition.

Dans la suite, nous nous placerons dans le modèle M1 d'ordre 1.

### NOMBRE ATTENDU D'OCCURRENCES

Soit  $W = w_1 w_2 \dots w_h$  un mot de longueur  $h$  sur l'alphabet  $\mathcal{A}$ . On note  $Y_i$  la variable aléatoire qui vaut 1 si une occurrence de  $W$  commence en position  $i$  dans la séquence  $S$  et 0 sinon. Le nombre  $N(W)$  d'occurrences du mot  $W$  dans la séquence  $S$  de longueur  $n$  est donc défini par

$$N(W) = \sum_{i=1}^{n-h+1} Y_i.$$

Le nombre moyen d'occurrences de  $W$  dans  $S$  sous le modèle M1 (ou espérance) vaut  $\mathbb{E}_1 N(W) = (n - h + 1)\mu_1(W)$  où  $\mu_1(W)$  est la moyenne des variables de Bernoulli  $Y_i$ , c'est-à-dire la probabilité d'observer le mot  $W$  à une position donnée dans une chaîne de Markov d'ordre 1. Cette probabilité s'écrit de la façon suivante en fonction des probabilités de transition et de la loi stationnaire :

$$\mu_1(W) = \mu(w_1) \prod_{j=1}^{h-1} \pi(w_j, w_{j+1}).$$

En pratique, les paramètres du modèle sont inconnus et estimés, comme on l'a vu plus haut, à partir de la séquence d'ADN observée ; cela nous permet d'obtenir un estimateur  $\hat{\mathbb{E}}_1(N(W))$  du comptage moyen, noté plus simplement  $\hat{N}_1(W)$ , donné par :

$$\hat{N}_1(W) = \frac{\prod_{j=1}^{h-1} N(w_j w_{j+1})}{\prod_{j=2}^{h-1} N(w_j)}.$$

Par exemple, le comptage moyen estimé sous le modèle M1 du mot atc vaut  $N(at)cN(tc)/N(t)$ .

### SIGNIFICATIVITÉ DU COMPTAGE

Voyons maintenant un peu plus en détail comment calculer ou approcher la  $p$ -valeur  $\mathbb{P}(N(W) \geq c(W))$  sous le modèle M1.

### Approximation gaussienne

Dans le cas d'un mot  $W$  fixé, l'approximation gaussienne du comptage  $N(W)$  permet de déterminer si l'écart entre  $N(W)$  et  $\hat{N}_1(W)$  (comptage estimé dans M1) est significativement grand en valeur absolue. En effet, lorsque l'on normalise cet écart par un estimateur de son écart type, on montre que la statistique  $U_1(W)$  ainsi formée :

$$U_1(W) = \frac{N(W) - \hat{N}_1(W)}{\hat{\sigma}_1(W)} \quad (1)$$

converge en loi vers une variable aléatoire gaussienne d'espérance 0 et de variance 1. Nous ne donnerons pas ici l'expression de  $\hat{\sigma}_1(W)$  mais faisons simplement remarquer qu'elle fait intervenir la structure d'auto-recouvrement du mot  $W$ .

La statistique  $U_1(W)$  nous permet ainsi d'évaluer la significativité de l'écart  $N(W) - \hat{N}_1(W)$  compte tenu de la fréquence des mots de longueur 2. En effet, il suffit de calculer la probabilité  $\mathbb{P}(X \geq U_1^{\text{obs}}(W))$  pour une variable aléatoire  $X$  distribuée suivant la loi gaussienne centrée réduite, et  $U_1^{\text{obs}}(W)$  calculée avec la valeur observée de  $N(W)$  dans la séquence. Ainsi lorsque

**Encadré 1**

## NORMALITÉ ASYMPTOTIQUE DU COMPTAGE

La normalité asymptotique de  $n^{-1/2}(N(W) - \mathbb{E}N(W))$  s'obtient par un théorème de limite centrale pour chaînes de Markov. Celle de  $n^{-1/2}(N(W) - \widehat{N}_1(W))$  en découle par la  $\delta$ -méthode puisque  $\widehat{N}_1(W)$  est une fonction de certains comptages, eux aussi asymptotiquement gaussiens. Cependant, cette méthode est trop fastidieuse pour nous donner la variance asymptotique. La variance de l'écart

$N(W) - \widehat{N}_1(W)$  n'est en effet pas égale à la variance de  $N(W)$  du fait du caractère aléatoire de l'estimateur  $\widehat{N}_1(W)$ . La variance asymptotique de  $n^{-1/2}(N(W) - \widehat{N}_1(W))$  est en fait égale à la limite de  $n^{-1}\text{Var}(N(W) | X_1, N(ab), a, b \in \mathcal{A})$  où  $\{X_1, N(ab), a, b \in \mathcal{A}\}$  est la statistique exhaustive du modèle M1.

$U_1^{\text{obs}}(W)$  est négative et grande en valeur absolue, le mot  $W$  est un mot exceptionnellement rare pour le modèle ; inversement, si la statistique  $U_1^{\text{obs}}(W)$  est positive et grande en valeur absolue,  $W$  est un mot exceptionnellement fréquent pour le modèle.

**Approximation par une loi de Poisson composée**

La méthode de Chen-Stein permet de mesurer l'erreur commise lorsque l'on approche une somme de variables aléatoires de Bernoulli dépendantes par une loi de Poisson. C'est ainsi une généralisation de l'approximation d'une loi binomiale par une loi de Poisson. La loi de Poisson étant la « loi des événements rares », il n'est pas surprenant de devoir ici se placer dans le cas où le mot  $W$  a un comptage attendu de l'ordre de 1 quand la longueur  $n$  de la séquence croît vers l'infini. Sous cette condition,

qui revient à considérer un mot dont la longueur est de l'ordre de  $\log n$ , on montre que l'approximation de la loi du comptage par la loi de Poisson de même moyenne n'est valable que pour des mots non auto-recouvrants. Pour les mots auto-recouvrants, les indicatrices d'occurrences  $Y_i$  ne peuvent donc pas être considérées comme indépendantes même asymptotiquement. Cela vient simplement du fait que les occurrences d'un mot auto-recouvrant ont tendance à former des paquets, ou « trains », d'occurrences chevauchantes. En fait, la méthode de Chen-Stein nous permet de montrer que le nombre de trains, noté  $\tilde{N}(W)$ , peut lui s'approcher par une variable de Poisson. De plus, les « tailles » des trains (nombres de « wagons »  $W$ ) sont indépendantes et de même loi (une loi géométrique dont le paramètre est connu et bien sûr lié à la structure d'auto-recouvrement du mot). Ainsi, en écrivant le comptage  $N(W)$  comme la somme sur les trains de  $W$  de la taille des trains :

**Encadré 2**

## MÉTHODE DE CHEN-STEIN

Cette méthode donne une majoration de l'erreur commise lorsque l'on remplace la loi d'une somme de  $n$  variables aléatoires de Bernoulli  $Y_i$  non indépendantes et de paramètre  $p_i$ , par la loi de Poisson de même espérance  $\lambda := \sum_{i=1}^n p_i$ . Cette erreur est mesurée en terme de distance en variation totale entre les deux lois ; cette distance se définit pour deux variables aléatoires discrètes  $N$  et  $Z$  par :

$$d_{VT}(\mathcal{L}(N), \mathcal{L}(Z)) := \sup_{A \subset \mathbb{N}} |\mathbb{P}(X \in A) - \mathbb{P}(Z \in A)|.$$

Soient donc  $N = \sum_{i=1}^n Y_i$  et  $Z$  une variable aléatoire de Poisson de paramètre  $\lambda$ . La borne de la distance en variation totale entre les lois de  $N$  et  $Z$  va s'exprimer en fonction du niveau de dépendance entre les variables de Bernoulli  $Y_i$  dont les indices font partie d'un certain voisinage (à définir)  $B_i$  de  $i$ .

Le théorème est le suivant :

$$d_{VT}(\mathcal{L}(N), \mathcal{L}(Z)) \leq (b_1 + b_2 + b_3)$$

avec

$$b_1 = \sum_{i=1}^n \sum_{j \in B_i} p_i p_j$$

$$b_2 = \sum_{i=1}^n \sum_{j \in B_i \setminus \{i\}} \mathbb{E}(Y_i Y_j)$$

$$b_3 = \sum_{i=1}^n \mathbb{E}|\mathbb{E}(Y_i - p_i | \sigma(Y_j, j \notin B_i))|.$$

$$N(W) = \sum_{j=1}^{\tilde{N}(W)} \{\text{taille du } j^{\text{ième}} \text{ train}\}$$

on obtient par définition une loi de Poisson composée comme loi limite. La  $p$ -valeur sera alors approchée par la queue de la loi de Poisson composée *ad hoc*.

loi de Poisson composée limite. Comme l'on s'y attendait théoriquement, la loi gaussienne est à éviter lorsque les mots sont de plus en plus longs, c'est-à-dire de plus en plus rares. De façon surprenante, la loi de Poisson composée semble donner de très bons résultats même pour des mots *a priori* non rares (encadré 3).

### Encadré 3

## COMPARAISON DES MÉTHODES

En pratique, l'utilisation de la loi exacte du comptage pour calculer les  $p$ -valeurs est souvent rédhibitoire compte tenu des longueurs de séquences d'ADN manipulées. A titre d'exemple, il faut 6 heures pour l'étude des mots de longueur 9 dans une séquence de seulement 50 000 bases sous le modèle M0 (le temps passe à 44 heures dans M1), et seulement une vingtaine de secondes en utilisant les lois limites gaussienne ou de Poisson composée. Il est alors important de juger des qualités des  $p$ -valeurs approchées calculées comme alternatives. La figure ci-contre montre que l'approche gaussienne (première colonne) est adaptée pour les mots courts mais devient très mauvaise au fur et à mesure que la longueur de mots augmente. La loi de Poisson composée (deuxième colonne) donne quant à elle de bons résultats. Une approximation de la  $p$ -valeur par des techniques de grandes déviations (non détaillées ici) semble aussi donner de bons résultats pour les mots exceptionnels. Un point important pour les biologistes est que quelle que soit la méthode utilisée, les mots sont quasiment classés dans le même ordre d'exceptionnalité. Cela leur permet, grâce à la loi gaussienne ou de Poisson composée, de dégager efficacement un lot de mots exceptionnels pour lesquels un calcul exact de la  $p$ -valeur peut être effectué.

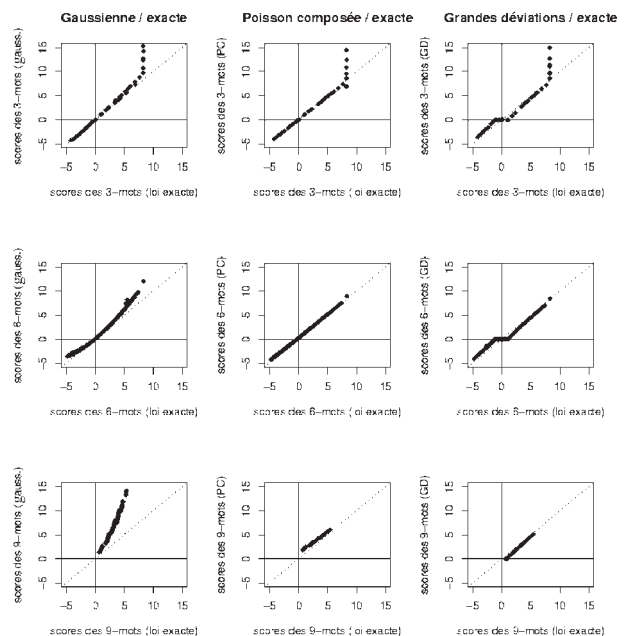


Figure - Comparaison des  $p$ -valeurs exactes (en abscisse) et des  $p$ -valeurs approchées (en ordonnée) obtenues sous le modèle M0 pour les mots de longueur 3 (ligne 1), 6 (ligne 2) et 9 (ligne 3) dans le génome complet du phage Lambda ( $n = 48\,502$ ). Les 3 colonnes correspondent successivement aux approches gaussienne, de Poisson composée et de grandes déviations. Les  $p$ -valeurs sont représentées sous la forme d'un score gaussien centré réduit.

### Comparaison des méthodes

Si la loi exacte du comptage n'est généralement pas accessible en pratique, il est important de pouvoir juger de la qualité des deux approximations. Outre une comparaison théorique des 3 lois, nous avons comparé, à partir de l'analyse d'une séquence d'ADN particulière, les  $p$ -valeurs obtenues en utilisant la loi exacte (en négligeant l'estimation des paramètres), la loi gaussienne limite et la

### INFLUENCE DU MODÈLE

Le caractère exceptionnel d'un mot dans une séquence est relatif à la quantité d'information prise en compte sur la séquence, à savoir au modèle choisi. C'est en effet le modèle qui détermine le comptage attendu, à savoir le comptage de référence. Changer de modèle peut alors modifier les résultats.

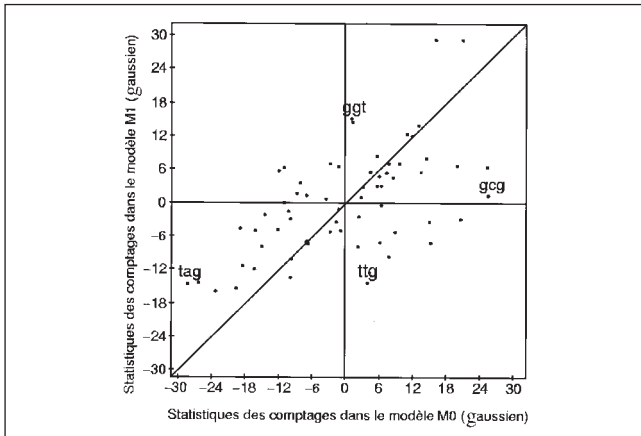


Figure 1 - Exceptionnalité des tri-nucléotides dans la séquence ECOMORI de *E. coli*, respectivement sous les modèles M0 (en abscisse) et M1 (en ordonnée).

En guise d'illustration, regardons la fréquence des tri-nucléotides (mots de longueur 3) dans une séquence de longueur 111 402 contenue dans le génome de *E. coli* (> 4,6 millions de bases) en se plaçant successivement dans les modèles M0 et M1. On va voir que les mots ne seront pas exceptionnels de la même façon dans les deux modèles, pour la simple raison que le modèle M1 prend en compte le biais éventuel de composition en di-nucléotides (mots de longueur 2) de la séquence, alors que le modèle M0 n'intègre que le biais de composition en bases.

On associe à chacun des 64 tri-nucléotides  $abc$  le couple  $(U_0(abc), U_1(abc))$ , représentant leurs statistiques asymptotiquement gaussiennes d'espérance 0 et d'écart type 1 (équation [1]) dans les modèles M0 et M1. Par conséquent, une forte valeur positive de  $U(abc)$  identifie un mot  $abc$  exceptionnellement fréquent, tandis qu'une forte valeur négative de  $U(abc)$  identifie un mot  $abc$  exceptionnellement rare.

La figure 1 représente les 64 tri-nucléotides  $abc$  par un point dont les coordonnées sont  $(U_0(abc), U_1(abc))$ . Tous les points n'étant pas alignés sur la bissectrice, les statistiques sont donc bien différentes lorsque l'on change de modèle ; le modèle choisi a par conséquent une importance dans l'interprétation des résultats. Certains mots peuvent conserver leur exceptionnalité en augmentant l'ordre du modèle (c'est le cas de  $tag$  qui est exceptionnellement rare dans M0 et M1) tandis que d'autres peuvent la perdre : c'est la contamination par les sous-mots. Prenons l'exemple de  $gcg$  ; si l'on tient compte uniquement de la composition en bases (M0),  $gcg$  est attendu 2 105 fois ; or il est présent 3 194 fois et l'écart est très significatif.  $gcg$  est donc exceptionnellement fréquent sous M0. Si maintenant on tient compte de la composition en di-nucléotides (M1),  $gcg$  est attendu 3 148 fois ce qui n'est pas significativement inférieur au comptage observé. Cette perte d'exceptionnalité en augmentant l'ordre du modèle traduit le

fait que la fréquence élevée de  $gcg$  est simplement due au fait qu'il est composé d'un ou deux mots de longueur 2 fréquents. En effet,  $gc$  (respectivement  $cg$ ) est exceptionnellement fréquent dans M0, mais est « normale-ment » suivi (respectivement précédé) d'un  $g$ .

Au contraire, l'exceptionnalité de certains mots peut être masquée dans des petits modèles (c'est le cas de  $ggt$  qui n'est pas exceptionnel compte tenu de la composition en bases mais devient significativement sur-représenté dans le modèle M1). C'est en général dû à des phénomènes de compensation entre les sous-mots. Le cas de  $ttg$  est encore plus surprenant car il est sur-représenté dans M0 (sans être particulièrement exceptionnel) : il est attendu 1 758 et apparaît 1 904 fois, alors que dans M1 il est finalement attendu 2 396 fois, et  $ttg$  est considéré comme exceptionnellement rare. Ici,  $tt$  et  $tg$  sont plutôt sur-représentés dans la séquence mais une contrainte semble indiquer qu'ils ne « doivent pas » être juxtaposés. Pourquoi ? C'est une question adressée aux biologistes...

A travers ces exemples, on s'aperçoit de l'utilité d'étudier la fréquence d'un mot dans plusieurs modèles plutôt que de se restreindre à un seul. On obtient ainsi une information très précise sur la structure de la séquence ou encore de son « vocabulaire ». Se placer dans le modèle d'ordre maximal est le meilleur moyen pour détecter si un mot est vraiment exceptionnel de par lui-même (c'est le cas par exemple de  $ggt$ ,  $ttg$  et  $tag$ ), mais il a l'inconvénient de masquer des mots qui seraient exceptionnels uniquement parce qu'ils contiennent un sous-mot exceptionnel (c'est le cas par exemple de  $gcg$ ).

#### EXEMPLE DE MOT EXCEPTIONNEL

Chez *E. coli*, la séquence  $gctggtgg$ , appelée Chi, interagit avec une enzyme, appelée RecBCD, capable de dégrader très efficacement l'ADN double brin (provenant par exemple d'une cassure du chromosome de la bactérie ou d'un virus l'ayant infecté). La séquence Chi module en fait les fonctions de RecBCD : lorsqu'elle n'est pas présente, la fonction « dégradation » de RecBCD est active et la molécule d'ADN est efficacement détruite. Si au contraire la séquence Chi est présente, celle-ci est reconnue par RecBCD et une fonction « réparation » est activée. Ce phénomène conduit les biologistes à envisager que Chi soit particulièrement fréquente sur le génome d'*E. coli* afin d'assurer la protection du génome et la réparation en cas de cassure. Au contraire, l'ADN d'un virus ne comporterait probablement pas de séquence Chi et serait donc dégradé dès son entrée dans la cellule, ce qui protégerait *E. coli*. Il s'agit donc de savoir si la séquence Chi est significativement fréquente sur le génome de la bactérie.

Nous avons donc analysé le génome complet de *E. coli*, pris dans le sens de la répllication (biais dans l'activité de Chi), long de 4 638 858 bases. La séquence

gctggtgg y est présente 762 fois. Le tableau ci-contre rassemble, pour chaque modèle d'ordre  $m \in \{0, \dots, 6\}$ , le comptage attendu  $\widehat{N}_m$  de ce mot, le carré  $\widehat{\sigma}_m^2$  du facteur de normalisation, la statistique asymptotiquement gaussienne  $U_m$  et le rang de cette statistique parmi celles des 65 536 mots de longueur 8 classées par ordre décroissant.

On s'aperçoit que quelque soit l'ordre du modèle choisi, la séquence Chi est significativement sur-représentée et figure toujours parmi les 5 mots de longueur 8 les plus exceptionnel-lement fréquents. La contrainte est donc forte pour que ce mot soit fréquent : la composition en mots de longueur 7 (M6) ne suffit pas à expliquer les 762 occurrences de Chi. Cela conduit à proposer qu'une telle répartition de la séquence Chi sur le génome a été sélectionnée au cours de l'évolution. Les résultats de l'analyse statistique semblent donc confirmer les résultats de l'analyse génétique qui accorde à la séquence Chi et à l'enzyme RecBCD, son partenaire, un rôle fondamental

dans un processus qui permet à la fois de réparer le génome propre de la bactérie et de dégrader l'ADN étranger.

$m$	$\widehat{N}_m$	$\widehat{\sigma}_m^2$	$U_m$	rang
0	85,9	85,8	72,96	3
1	84,9	84,8	73,54	1
2	206,8	203,9	38,88	1
3	355,5	338,9	22,08	5
4	355,3	314,4	22,94	2
5	420,9	298,0	19,76	1
6	610,1	203,3	10,65	3

**Tableau 1** - Statistiques de gctggtgg dans le génome de E. coli sous différents modèles  $M_m$ .

## POUR EN SAVOIR PLUS

**Arratia (R.), Goldstein (L.), Gordon (L.),** « Two moments suffice for Poisson approximations: the Chen-Stein method », *Ann. Prob.*, 17, 9-25, 1989.

**Nuel (G.),** « Grandes déviations et chaînes de Markov pour l'étude des mots exceptionnels dans les séquences biologiques », *thèse de l'Université d'Evry*, 2001.

**Prum (B.), Rodolphe (F.), de Turckheim (E.),** « Finding words with unexpected frequencies in DNA sequences », *J. R. Statist. Soc. B*, 57, 205-220, 1995.

**Robin (S.), Daudin (J.-J.),** « Exact distribution of word occurrences in a random sequence of letters », *J. Appl. Prob.*, 36, 179-193, 1999.

**Robin (S.), Schbath (S.),** « Numerical comparison of several approximations of the word count distribution in random sequences », *J. Comp. Biol.*, 8, 349-359, 2001.

**Schbath (S.), Prum (B.), de Turckheim (E.),** « Exceptional motifs in different Markov chain models for a statistical analysis of DNA sequences », *J. Comp. Biol.*, 2, 417-437, 1995.

**Schbath (S.),** « Compound Poisson approximation of word counts in DNA sequences », *ESAIM: Prob. Stat.*, 1, 1-16, 1995.

# Graphes à grand tour de taille

**Le tour de taille d'un graphe est la longueur du plus petit circuit. Si le graphe modélise un réseau de transmission de l'information, il est intéressant d'avoir le tour de taille le plus grand possible, afin d'éliminer les redondances. Pour un graphe régulier, un argument de comptage élémentaire montre que le tour de taille est au plus logarithmique en le nombre de sommets. Mais il existe des familles de graphes réguliers où le tour de taille croît vraiment comme le logarithme du nombre de sommets. Le but de l'article est de donner la construction de celle de ces familles qui réalise le taux de croissance du tour de taille le plus rapide, parmi tous les taux de croissance connus.**

Dans cet article, il sera question de graphes finis, simples (c'est-à-dire sans boucle ni arête multiple), connexes, et  $k$ -réguliers (c'est-à-dire, tout sommet à exactement  $k$  voisins). Un exemple célèbre est donné à la figure 1 : c'est le graphe de Petersen, qui est 3-régulier.

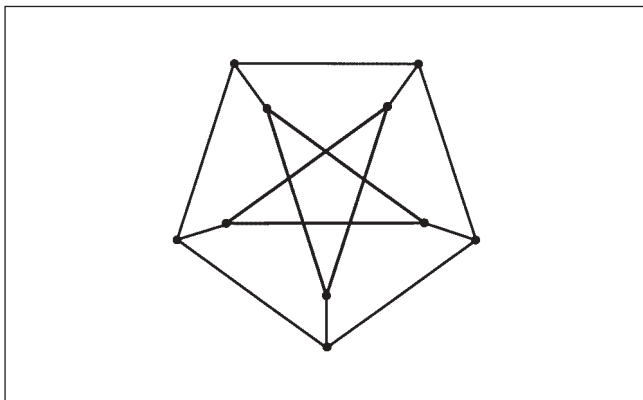


Figure 1

Le tour de taille d'un graphe  $X$  est la longueur du plus petit circuit de  $X$  (on dit aussi *maille*, ou *systole*<sup>1</sup>) : on le note  $g(X)$ .

Pour un graphe  $X$   $k$ -régulier, connexe, fini, il existe une relation simple entre le tour de taille  $g = g(X)$  et le nombre de sommets  $|X|$ . Notons  $r = \left\lfloor \frac{g-1}{2} \right\rfloor$  le plus grand entier strictement inférieur à  $\frac{g}{2}$ . Fixons un sommet  $x_0 \in X$ , et considérons la boule fermée  $B_{\leq r}(x_0)$  de centre  $x_0$  et de rayon  $r$ . Comme  $r < g/2$ , cette boule ne peut pas contenir de circuit ; en d'autres termes, le graphe induit par  $X$  sur  $B_{\leq r}(x_0)$ , est un arbre (figure 2).

<sup>1</sup> En anglais : « girth » ; en allemand : « taillenweite ».

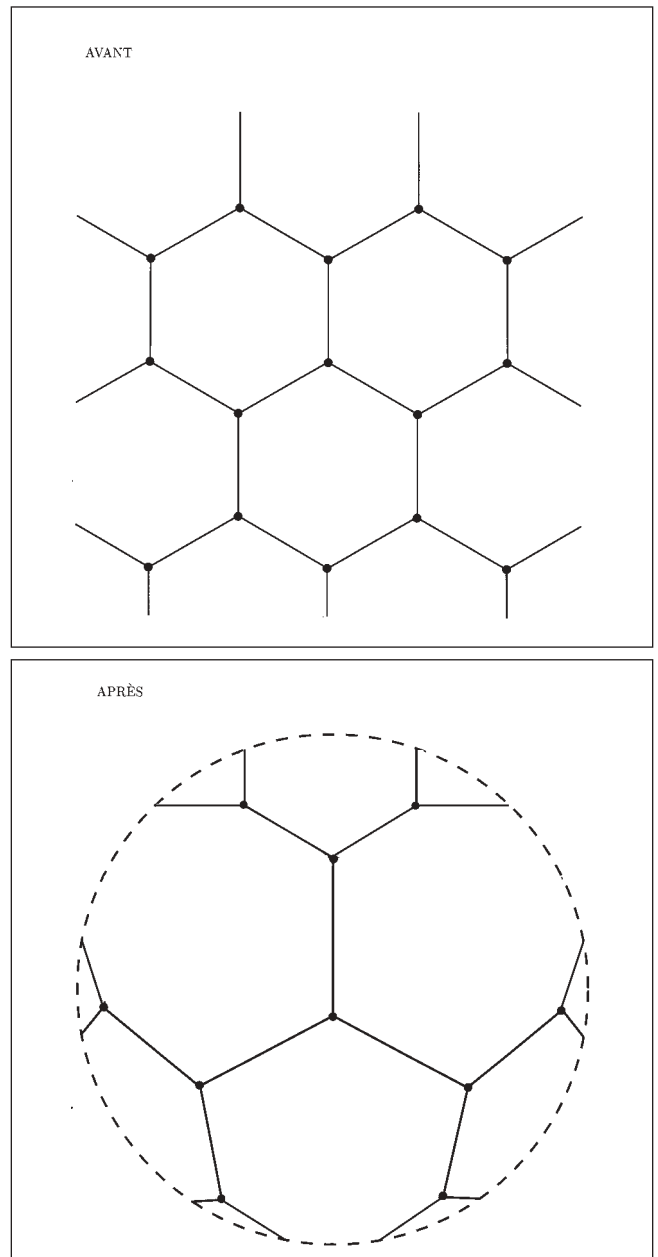


Figure 2



Le nombre de sommets de la boule  $B_{\leq r}(x_0)$  est facile à estimer : on additionne le nombre de sommets à distance 0 de  $x_0$ , le nombre de sommets à distance 1, le nombre de sommets à distance 2, etc. Comme le graphe  $X$  est  $k$ -régulier, cela donne :

$$|B_{\leq r}(x_0)| = 1 + k + k(k-1) + k(k-1)^2 + \dots + k(k-1)^{r-1} = \frac{k(k-1)^r - 2}{k-2}.$$

Ecrivons maintenant l'inégalité<sup>2</sup> triviale  $|B_{\leq r}(x_0)| \leq |X|$ . En passant au logarithme en base  $k-1$ , on obtient la relation recherchée :

$$\left\lceil \frac{g(X) - 1}{2} \right\rceil \leq \log_{k-1} |X| + \log_{k-1} \left\lceil \frac{k-2 + \frac{2}{|X|}}{k} \right\rceil.$$

Cette relation prend une forme particulièrement simple si, au lieu de considérer un graphe  $X$ , on considère une famille  $(X_n)_{n \geq 1}$  de graphes  $k$ -réguliers, connexes, finis, avec  $|X_n| \rightarrow +\infty$  pour  $n \rightarrow \infty$  :

$$g(X_n) \leq (2 + o(1)) \log_{k-1} |X_n| \quad (1)$$

(ici  $o(1)$  est une quantité qui tend vers 0 pour  $n \rightarrow \infty$ ).

L'intérêt de considérer des familles de graphes vient de la théorie des circuits de communication : un graphe modélise un réseau de communication, les sommets représentant les utilisateurs (émetteurs/récepteurs d'informations), les arêtes représentant les canaux le long desquels l'information se propage. La condition  $\lim_{n \rightarrow \infty} |X_n| = +\infty$  correspond au désir d'avoir des modèles de réseaux arbitrairement grands. L'exigence de  $k$ -régularité est de nature économique : en effet, le meilleur réseau de communication sur  $m$  sommets est donné par le graphe complet, où tout sommet est connecté à tout autre ; mais le nombre d'arêtes est  $\frac{m(m-1)}{2}$ , il est quadratique en  $m$ . En revanche, pour notre famille  $(X_n)_{n \geq 1}$  de graphes  $k$ -réguliers, le nombre d'arêtes de  $X_n$  est  $\frac{k|X_n|}{2}$  ; ce nombre croît donc linéairement avec  $|X_n|$ . Dans ce contexte, il est intéressant d'avoir le tour de taille le plus grand possible : le fait que les circuits soient longs veut dire qu'il y aura peu de retours de l'information, c'est-à-dire peu de redondances.

<sup>2</sup> Pour le graphe de Petersen, on a l'égalité  $B_{\leq r}(x_0) = X$ , mais c'est exceptionnel !

**Définition.** Soit  $(X_n)_{n \geq 1}$  une famille de graphes  $k$ -réguliers connexes, finis, avec  $\lim_{n \rightarrow \infty} |X_n| = +\infty$ . Nous dirons que  $(X_n)_{n \geq 1}$  est une famille à grand tour de taille s'il existe  $C > 0$  tel que

$$g(X_n) \geq (C + o(1)) \log_{k-1} |X_n| \quad \text{pour tout } n \geq 1.$$

Par l'inégalité (1), on a nécessairement  $C \leq 2$ . Une famille est à grand tour de taille si le tour de taille est de l'ordre du logarithme du nombre de sommets. Il n'est pas du tout évident que de telles familles existent. En effet, vu l'erreur commise dans la comparaison entre  $B_{\leq r}(x_0)$  et  $X$ , on pourrait penser que  $|X|$  est en général bien plus grand que  $|B_{\leq r}(x_0)|$ . Il est donc assez surprenant que de telles familles de graphes existent bel et bien : cela a été démontré en 1962 par Erdős et Sachs : grâce à des méthodes non constructives, ils démontrent l'existence de familles  $(X_n)_{n \geq 1}$  avec  $g(X_n) \geq \log_{k-1} |X_n|$  (c'est-à-dire  $C = 1$ ). Une jolie construction élémentaire, complètement explicite, a ensuite été donnée par Margulis en 1982 ; malheureusement, elle ne donne que  $C = \frac{2 \log 3}{3 \log(1 + \sqrt{2})} \simeq 0,831$ . Notre but dans cet article est de présenter une preuve élémentaire<sup>3</sup> du résultat suivant, obtenu indépendamment en 1988 par Lubotzky, Phillips, Sarnak d'une part, et Margulis d'autre part.

**Théorème 1.** Soient  $p, q$  des nombres premiers impairs distincts, avec  $p \equiv 1 \pmod{4}$  et  $\left(\frac{p}{q}\right) = -1$  (c'est-à-dire que  $p$  n'est pas un carré modulo  $q$ ). Il existe une famille  $(X^{p,q})$ , construite explicitement, de graphes  $(p+1)$ -réguliers sur  $q(q^2-1)$  sommets, avec  $g(X^{p,q}) \geq \left(\frac{4}{3} + o(1)\right) \log_p |X^{p,q}|$ .

Les graphes  $X^{p,q}$  seront des graphes de Cayley du groupe fini  $\text{PGL}_2(q)$ , d'ordre  $\frac{q(q-1)}{2}$ , par rapport à une partie génératrice à  $p+1$  éléments construite à partir du théorème des quatre carrés de Jacobi.

A notre connaissance, la constante  $C = \frac{4}{3}$  du théorème 1 détient le record du monde. La preuve ci-dessous est tirée d'un travail en commun avec Davidoff et Sarnak.

<sup>3</sup> La preuve originale utilisait les groupes algébriques sur les adèles, en particulier le théorème d'approximation forte de Kneser.

RAPPELS

Graphes de Cayley

Les graphes que nous construirons seront des graphes de Cayley. Rappelons rapidement cette notion.

Soit  $\Gamma$  un groupe (fini ou infini) et  $S$  une partie finie de  $\Gamma$ . Nous supposons que  $S$  ne contient pas le neutre 1 de  $\Gamma$  et que  $S$  est symétrique, c'est-à-dire stable par le passage à l'inverse. Le *graphe de Cayley*  $\mathcal{G}(\Gamma, S)$  est le graphe dont l'ensemble des sommets est  $\Gamma$  et dont l'ensemble des arêtes est formé des paires  $\{x, y\}$  pour lesquelles il existe  $s \in S$  tel que  $y = xs$ . Notons que cette relation d'adjacence est symétrique (car  $S = S^{-1}$ ) et que le graphe  $\mathcal{G}(\Gamma, S)$  est simple (car  $1 \notin S$ ).

La figure 3 donne différents exemples de graphes de Cayley du groupe additif  $\Gamma = \mathbb{Z}/6\mathbb{Z}$  (groupe cyclique d'ordre 6).

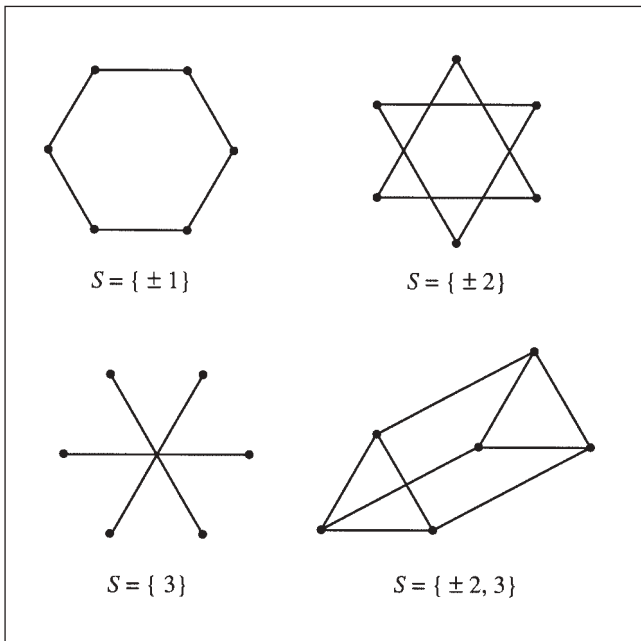


Figure 3

Les propriétés principales d'un graphe de Cayley sont les suivantes :

- $\mathcal{G}(\Gamma, S)$  est  $k$ -régulier, avec  $k = |S|$  ;
- $\Gamma$  agit par automorphismes sur  $\mathcal{G}(\Gamma, S)$ , transitivement sur les sommets (grâce aux multiplications gauches de  $\Gamma$ ) ;
- $\mathcal{G}(\Gamma, S)$  est connexe si et seulement si  $S$  engendre  $\Gamma$  (en effet :  $\mathcal{G}(\Gamma, S)$  est connexe si et seulement si tout sommet peut être relié au sommet  $1 \in \Gamma$ , si et seulement si tout élément de  $\Gamma$  s'écrit comme un produit d'éléments de  $S$ ).

Sommes de 4 carrés

Partons du théorème des 4 carrés de Jacobi (voir Weil et Davidoff, Sarnak et Valette pour les preuves élémentaires) : si  $p$  est premier, il y a  $8(p + 1)$  manières d'écrire  $p$  comme somme de 4 carrés d'entiers :

$$|\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : x_0^2 + x_1^2 + x_2^2 + x_3^2 = p\}| = 8(p + 1).$$

Supposons dorénavant  $p \equiv 1 \pmod{4}$ . En réduisant  $x_0^2 + x_1^2 + x_2^2 + x_3^2 = p \pmod{4}$ , et en se rappelant que les carrés modulo 4 sont 0 et 1, on voit qu'exactement un des  $x_i$  est impair et les autres pairs. Ainsi

$$|\{(x_0, x_1, x_2, x_3) \in \mathbb{Z}^4 : x_0^2 + x_1^2 + x_2^2 + x_3^2 = p, x_0 \text{ impair, } x_0 > 0\}| = p + 1. \quad (2)$$

Quaternions

Si  $R$  est un anneau commutatif à unité, nous noterons  $\mathbb{H}(R)$  l'anneau des *quaternions de Hamilton* à coefficients dans  $R$

$$\mathbb{H}(R) = \{a_0 + a_1 i + a_2 j + a_3 k : a_0, a_1, a_2, a_3 \in R\}$$

où les symboles  $i, j, k$  sont soumis aux relations usuelles :

$$i^2 = j^2 = k^2 = -1, ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Si  $\alpha = a_0 + a_1 i + a_2 j + a_3 k$  est un quaternion, nous définissons le *quaternion conjugué*  $\bar{\alpha} = a_0 - a_1 i - a_2 j - a_3 k$ , ainsi que la *norme* :

$$N(\alpha) = \bar{\alpha} \alpha = \alpha \bar{\alpha} = a_0^2 + a_1^2 + a_2^2 + a_3^2.$$

Notons  $\mathbb{F}_q$  le corps fini à  $q$  éléments ( $q$  impair). Rappelons que, dans  $\mathbb{F}_q$ , l'équation  $1 + x^2 + y^2 = 0$  possède toujours au moins une solution (pour le voir, posons  $A_+ = \{1 + x^2 : x \in \mathbb{F}_q\}$ ,  $A_- = \{-y^2 : y \in \mathbb{F}_q\}$  : ces deux sous-ensembles de  $\mathbb{F}_q$  ont tous deux  $\frac{q+1}{2}$  éléments, soit plus de la moitié des éléments de  $\mathbb{F}_q$ , donc leur intersection est non vide : il existe donc  $x, y \in \mathbb{F}_q$  tels que  $1 + x^2 = -y^2$ ).

L'anneau de quaternions  $\mathbb{H}(\mathbb{F}_q)$  est isomorphe à l'anneau  $M_2(\mathbb{F}_q)$  des matrices  $2 \times 2$  à coefficients dans  $\mathbb{F}_q$ . Cet isomorphisme n'est pas canonique, mais dépend du choix des deux éléments  $x, y$  tels que  $1 + x^2 + y^2 = 0$  dans  $\mathbb{F}_q$ . Choisissons ces éléments une fois pour toutes, et posons

$$\begin{aligned} \psi_q : \mathbb{H}(\mathbb{F}_q) &\rightarrow M_2(\mathbb{F}_q) : \\ & a_0 + a_1 i + a_2 j + a_3 k \\ \mapsto & \begin{pmatrix} a_0 + a_1 x + a_3 y & -a_1 y + a_2 + a_3 x \\ -a_1 y - a_2 + a_3 x & a_0 - a_1 x - a_3 y \end{pmatrix}. \end{aligned}$$

On vérifie que  $\psi_q$  est un isomorphisme d'anneaux, tel que

$$\det \psi_q(\alpha) = N(\alpha) \quad (\alpha \in \mathbb{H}(\mathbb{F}_q)) \quad (3)$$

De plus  $\psi_q(\alpha \bar{\alpha}) = \psi_q(\bar{\alpha} \alpha)$  est une matrice scalaire.

### Groupes finis

Notons  $GL_2(q)$  le groupe des matrices  $2 \times 2$ , inversibles, à coefficients dans  $\mathbb{F}_q$ . L'ordre de  $GL_2(q)$  est

$$|GL_2(q)| = q(q-1)(q^2-1)$$

(en effet, on peut choisir de  $q^2-1$  façons la première colonne d'une matrice inversible et de  $q^2-q = q(q-1)$  façons sa deuxième colonne, linéairement indépendante de la première).

Notons  $SL_2(q)$  le sous-groupe des matrices de déterminant 1. On a donc  $SL_2(q) = \text{Ker}[\det : GL_2(q) \rightarrow \mathbb{F}_q^\times]$  et par conséquent

$$|SL_2(q)| = q(q^2-1).$$

Notons enfin  $PGL_2(q)$  le quotient de  $GL_2(q)$  par son centre, formé des matrices scalaires. On a donc

$$|PGL_2(q)| = q(q^2-1).$$

Notons  $\varphi_q : GL_2(q) \rightarrow PGL_2(q)$  l'application-quotient, et posons  $PSL_2(q) = \varphi_q(SL_2(q))$ . On a donc

$$|PSL_2(q)| = \begin{cases} q(q^2-1) & \text{si } q \text{ est pair} \\ \frac{q(q^2-1)}{2} & \text{si } q \text{ est impair} \end{cases}$$

Remarquons que, pour  $A \in GL_2(q)$ , on a  $\varphi_q(A) \in PSL_2(q)$  si et seulement si  $\det A$  est un carré dans  $\mathbb{F}_q$ .

### LES GRAPHES $X^{p,q}$

Comme en (2), considérons les  $p+1$  solutions de

$$x_0^2 + x_1^2 + x_2^2 + x_3^2 = p, \quad x_0 \text{ impair}, \quad x_0 > 0.$$

A chacune de ces solutions, associons le quaternion entier

$$x_0 + x_1 i + x_2 j + x_3 k.$$

Cela fournit un ensemble  $S_p$  de  $p+1$  quaternions dans  $\mathbb{H}(\mathbb{Z})$ . Considérons la réduction *modulo*  $q$

$$\tau_q : \mathbb{H}(\mathbb{Z}) \rightarrow \mathbb{H}(\mathbb{F}_q)$$

composée avec l'isomorphisme

$$\psi_q : \mathbb{H}(\mathbb{F}_q) \rightarrow M_2(\mathbb{F}_q).$$

On a, pour  $\alpha \in S_p$  :

$$\det(\psi_q(\tau_q(\alpha))) \equiv N(\alpha) = p \pmod{q},$$

donc  $\psi_q(\tau_q(S_p))$  est contenu dans le groupe  $GL_2(q)$  des matrices inversibles de  $M_2(\mathbb{F}_q)$ . Notons que  $S_p$  est stable par le passage au conjugué  $\alpha \mapsto \bar{\alpha}$ . Comme  $\psi_q(\tau_q(\bar{\alpha}\alpha))$  est une matrice scalaire, cela suggère de passer au quotient par les matrices scalaires, donc de travailler dans le quotient  $PGL_2(q)$ .

On a alors, pour  $\alpha \in S_p$  :

$$\varphi_q \circ \psi_q \circ \tau_q(\alpha \bar{\alpha}) = 1$$

ce qui montre que  $S_{p,q} = (\varphi_q \circ \psi_q \circ \tau_q)(S_p)$  est une partie symétrique de  $PGL_2(q)$ . Il est facile de voir que, si  $q$  est assez grand par rapport à  $p$  (c'est-à-dire  $q > 2\sqrt{p}$ ), alors  $(\varphi_q \circ \psi_q \circ \tau_q)|_{S_p}$  est injective et  $1 \notin S_{p,q}$ .

Si  $\left(\frac{p}{q}\right) = 1$  (c'est-à-dire si  $p$  est un carré *modulo*  $q$ ),

alors  $S_{p,q} \subseteq PSL_2(q)$ . Nous posons  $X^{p,q} = \mathcal{G}(PSL_2(q), S_{p,q})$  : c'est un graphe  $(p+1)$ -régulier, à  $\frac{q(q^2-1)}{2}$  sommets.

Si  $\left(\frac{p}{q}\right) = -1$  (c'est-à-dire si  $p$  n'est pas un carré *modulo*  $q$ ), alors  $S_{p,q} \subseteq PGL_2(q) \setminus PSL_2(q)$ , et nous posons  $X^{p,q} = \mathcal{G}(PGL_2(q), S_{p,q})$  : c'est un graphe  $(p+1)$ -régulier à  $q(q^2-1)$  sommets.

Nous devons maintenant montrer que  $X^{p,q}$  est connexe, c'est-à-dire montrer que  $S_{p,q}$  engendre

$$\begin{cases} PSL_2(q) & \text{si } \left(\frac{p}{q}\right) = 1 \\ PGL_2(q) & \text{si } \left(\frac{p}{q}\right) = -1 \end{cases}$$

Après cela, il nous restera à estimer le tour de taille de  $X^{p,q}$ . Pour traiter ces deux problèmes, nous allons construire une famille de graphes  $Y^{p,q}$ , connexes par construction, et les comparer aux  $X^{p,q}$ .

LES GRAPHES  $Y^{p,q}$

Soit  $\Lambda'(2)$  le sous-ensemble suivant de  $\mathbb{H}(\mathbb{Z})$  :

$$\begin{aligned} \Lambda'(2) &= \{\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}(\mathbb{Z}) : \\ N(\alpha) &= p^r \ (r \in \mathbb{N}), \ \alpha \text{ impair}\}. \end{aligned}$$

Remarquons que  $\Lambda'(2)$  est un monoïde multiplicatif contenant  $S_p$ . En particulier  $\Lambda'(2)$  contient les mots sur l'alphabet  $S_p$ . Nous dirons qu'un tel mot est réduit s'il ne contient aucun sous-mot de la forme  $\alpha \bar{\alpha}$  ou  $\bar{\alpha} \alpha$  ( $\alpha \in S_p$ ).

**Théorème 2 (Dickson 1922).** *Écrivons  $S_p = \{\alpha_1, \dots, \alpha_{\frac{p+1}{2}}, \bar{\alpha}_1, \dots, \bar{\alpha}_{\frac{p+1}{2}}\}$ . Tout élément  $\alpha \in \Lambda'(2)$ , avec  $N(\alpha) = p^r$ , s'écrit de façon unique  $\alpha = \pm p^\ell w_m$ , où  $w_m$  est un mot réduit sur  $S_p$  et  $2\ell + m = r$ .*

Pour une preuve de ce résultat, voir Dickson (1922) et Davidoff, Sarnak et Valette.

Le théorème de Dickson voit pointer un groupe libre, plus exactement le groupe libre sur les  $\frac{p+1}{2}$  générateurs  $\alpha_1, \dots, \alpha_{\frac{p+1}{2}}$ . Pour faire apparaître celui-ci explicitement, passons au quotient  $\Lambda'(2)$  par une relation d'équivalence : pour  $\alpha, \beta \in \Lambda'(2)$  :  $\alpha \sim \beta$  s'il existe des naturels  $m, k$  tels que  $p^m \alpha = \pm p^k \beta$ . Notons  $[\alpha]$  la classe de  $\alpha$ . Le théorème de Dickson se reformule en disant que  $\Lambda(2) = \Lambda'(2) / \sim$  est le groupe libre  $\mathbb{L}_{\frac{p+1}{2}}$  sur les générateurs  $[\alpha_1], \dots, [\alpha_{\frac{p+1}{2}}]$ .

La réduction  $\tau_q$  modulo  $q$  envoie  $\Lambda'(2)$  dans le groupe multiplicatif  $\mathbb{H}(\mathbb{F}_q)^\times$  de  $\mathbb{H}(\mathbb{F}_q)$ . Notons  $Z(\mathbb{H}(\mathbb{F}_q)^\times)$  le centre de  $\mathbb{H}(\mathbb{F}_q)^\times$ . L'homomorphisme de monoïdes  $\tau_q : \Lambda'(2) \rightarrow \mathbb{H}(\mathbb{F}_q)^\times$  induit par passage au quotient un homomorphisme de groupes

$$\Pi_q : \Lambda(2) \rightarrow \mathbb{H}(\mathbb{F}_q)^\times / Z(\mathbb{H}(\mathbb{F}_q)^\times).$$

A nouveau  $\Pi_q|_{S_p}$  est injectif si  $q$  est assez grand par rapport à  $p$  ( $q > 2\sqrt{p}$  marche) et nous définissons  $Y^{p,q}$  comme le graphe de Cayley de l'image de  $\Pi_q$  par rapport à  $S_p$  :

$$Y^{p,q} = \mathcal{G}(\text{Im } \Pi_q, S_p).$$

Par construction,  $Y^{p,q}$  est un graphe  $(p+1)$ -régulier connexe. Comparons la construction de  $X^{p,q}$  et celle de  $Y^{p,q}$  au moyen d'un diagramme commutatif. Pour cela, remarquons que l'isomorphisme  $\psi_q : \mathbb{H}(\mathbb{F}_q)^\times \rightarrow \text{GL}_2(q)$  envoie  $Z(\mathbb{H}(\mathbb{F}_q)^\times)$  sur les matrices scalaires et induit donc un isomorphisme

$$\Psi_q : \mathbb{H}(\mathbb{F}_q)^\times / Z(\mathbb{H}(\mathbb{F}_q)^\times) \rightarrow \text{PGL}_2(q).$$

On a alors le diagramme commutatif :

$$\begin{array}{ccccc} \Lambda'(2) \supset S_p & \xrightarrow{\tau_q} & \mathbb{H}(\mathbb{F}_q)^\times & \xrightarrow{\psi_q} & \text{GL}_2(q) \\ \downarrow & & \downarrow & & \downarrow \varphi_q \\ \Lambda(2) & \xrightarrow{\Pi_q} & \mathbb{H}(\mathbb{F}_q)^\times / Z(\mathbb{H}(\mathbb{F}_q)^\times) & \xrightarrow{\Psi_q} & \text{PGL}_2(q) \supseteq Q_{p,q}. \end{array}$$

Ce diagramme montre déjà que  $Y^{p,q}$  est une composante connexe de  $X^{p,q}$ . L'inconvénient de  $Y^{p,q}$  est que nous ne connaissons pas *a priori* son nombre de sommets (contrairement à  $X^{p,q}$ ). Mais il a l'avantage d'être donné comme quotient d'un arbre (l'arbre du groupe libre  $\Lambda(2) \simeq \mathbb{L}_{\frac{p+1}{2}}$ ) d'avoir ainsi un tour de taille facile à estimer.

Notons  $\Lambda(2q)$  le noyau de l'homomorphisme  $\Pi_q$ . On peut penser à  $\Lambda(2q)$  comme à un sous-groupe de congruence dans  $\Lambda(2)$ . Il est facile de vérifier que

$$\Lambda(2q) = \{[\alpha] \in \Lambda(2) : \alpha = a_0 + a_1 i + a_2 j + a_3 k, \ (4) \text{ divise } a_1, a_2, a_3\}.$$

**Proposition 1.**  *$g(Y^{p,q}) \geq 2 \log_p q$  ; de plus, si  $\left(\frac{p}{q}\right) = -1$ , alors  $g(Y^{p,q}) \geq 4 \log_p q - \log_p 4$ .*

**Preuve.** Notons  $g$  pour  $g(Y^{p,q})$ . Soient  $x_0, x_1, \dots, x_g = x_0$  les sommets d'un circuit de longueur  $g$  dans  $Y^{p,q}$ . Comme  $Y^{p,q}$  est un graphe de Cayley, nous pouvons (quitte à traduire dans  $\text{Im } \Pi_q$ ) supposer que  $x_0 = 1$ . En relevant ce chemin en un chemin issu de l'origine dans l'arbre de Cayley de  $\Lambda(2)$ , nous voyons que

$$g = \min \{ \|\alpha\|_{S_p} : [\alpha] \in \Lambda(2q), [\alpha] \neq 1 \},$$

où  $\|\cdot\|_{S_p}$  désigne la longueur des mots par rapport à  $S_p$  dans le groupe libre  $\Lambda(2)$ . Soit donc  $\alpha = a_0 + a_1 i + a_2 j + a_3 k \in \Lambda'(2)$ , tel que  $[\alpha] \in \Lambda(2q)$  et  $\|\alpha\|_{S_p} = g$ . En prenant les normes, on a

$$p^g = a_0^2 + a_1^2 + a_2^2 + a_3^2$$

et au moins un des nombres  $a_1, a_2, a_3$  est non nul, car  $[\alpha] \neq 1$ . D'autre part,  $q$  divise  $a_1, a_2, a_3$  par (4). Donc  $p^g \geq q^2$ , c'est-à-dire  $g \geq 2 \log_p q$ .

Si  $\left(\frac{p}{q}\right) = -1$ , comme  $p^g \equiv a_0^2 \pmod{q}$ , on voit d'abord que  $g$  est pair, disons  $g = 2h$ . Remarquons que l'on a en fait

$$p^{2h} \equiv a_0^2 \pmod{q^2}$$

ce qui implique (pas complètement trivialement, car on travaille modulo  $q^2$ ) :

$$p^h \equiv \pm a_0 \pmod{q^2}.$$

D'autre part,  $a_0^2 \leq p^g$ , donc  $|a_0| \leq p^{g/2}$ . Supposons par l'absurde  $g < 4 \log_p q - \log_p 4$ , c'est-à-dire  $p^h < \frac{q^2}{2}$ . Alors  $|p^h \mp a_0| < q^2$ . De la congruence précédente, nous tirons  $p^h = \pm a_0$ . Alors  $p^g = a_0^2$ , ce qui implique  $a_1 = a_2 = a_3 = 0$  : c'est la contradiction désirée.

Notons que cette proposition, jointe à l'inégalité (1), donne la borne inférieure

$$|Y^{p,q}| = |\text{Im } \Pi_q| \geq q. \quad (5)$$

### PREUVE DU THÉORÈME 1

Le théorème 1 résulte de la proposition suivante :

**Proposition 2.** Si  $q > \sqrt{2} p^8$ , alors  $X^{p,q}$  est connexe [et donc  $X^{p,q} \simeq Y^{p,q}$ , et :

$$\text{si } \left(\frac{p}{q}\right) = 1 : \quad g(X^{p,q}) \geq \frac{2}{3} \log_p |X^{p,q}|$$

$$\text{si } \left(\frac{p}{q}\right) = -1 : \quad g(X^{p,q}) \geq \left(\frac{4}{3} + o(1)\right) \log_p |X^{p,q}|.$$

**Preuve.** Nous devons montrer que  $S_{p,q}$  engendre

$$\begin{cases} \text{PSL}_2(q) & \text{si } \left(\frac{p}{q}\right) = 1 \\ \text{PGL}_2(q) & \text{si } \left(\frac{p}{q}\right) = -1. \end{cases}$$

Notons  $\langle S_{p,q} \rangle$  le sous-groupe engendré par  $S_{p,q}$ , et posons

$$H = \langle S_{p,q} \rangle \cap \text{PSL}_2(q).$$

Pour  $g, h \in \text{PSL}_2(q)$ , notons  $[g, h] = g h g^{-1} h^{-1}$  le commutateur de  $g$  et  $h$ . Nous allons utiliser une propriété des sous-groupes de  $\text{PSL}_2(q)$ , encore due à Dickson :

**Théorème 3 (Dickson 1901).** Soit  $q$  un nombre premier,  $q \geq 7$ . Soit  $H$  un sous-groupe propre de  $\text{PSL}_2(q)$ . Si  $|H| > 60$ , alors  $H$  est métabélien, c'est-à-dire  $[[g_1, g_2], [g_3, g_4]] = 1$  pour tous  $g_1, g_2, g_3, g_4 \in H$ .

Pour une preuve de ce résultat, voir Dickson (1958) et Davidoff, Sarnak et Valette. La preuve du théorème 1 continue alors comme suit. Supposons par l'absurde que  $S_{p,q}$  n'engendre pas ce qu'il doit engendrer, ce qui revient à dire que  $H$  est un sous-groupe propre de  $\text{PSL}_2(q)$ . Remarquons que  $|H| \geq q > 60$ , par (5). Nous avons vu d'autre part que le graphe de Cayley  $\mathcal{G}(\langle S_{p,q} \rangle, S_{p,q})$  est isomorphe à  $Y^{p,q}$ . Considérons deux cas :

a) Si  $\left(\frac{p}{q}\right) = 1$ , alors la relation  $[[g_1, g_2], [g_3, g_4]] = 1$ , appliquée à quatre éléments de  $S_{p,q}$ , fournit un circuit de longueur 16 dans  $Y^{p,q}$ . Nous obtenons, grâce à la proposition 1 :

$$2 \log_p q \leq g(Y^{p,q}) \leq 16$$

c'est-à-dire  $q \leq p^8$ , une contradiction.

b) Si  $\left(\frac{p}{q}\right) = -1$ , alors la relation  $[[g_1, g_2], [g_3, g_4]] = 1$ , appliquée à quatre carrés d'éléments de  $S_{p,q}$ , fournit un circuit de longueur 32 dans  $Y^{p,q}$ . Nous obtenons, par la proposition 1 :

$$4 \log_p q - \log_p 4 \leq g(Y^{p,q}) \leq 32$$

c'est-à-dire  $q \leq \sqrt{2} p^8$ , à nouveau une contradiction.

**Remarques.** 1) Dans les articles originaux de Lubotzky, Phillips et Sarnak et de Margulis (1988) la connexité de  $X^{p,q}$  est démontrée pour  $q > 2\sqrt{p}$ , ce qui est évidemment meilleur que notre hypothèse de la proposition 2.

2) Si  $\left(\frac{p}{q}\right) = -1$ , Biggs et Boshier ont démontré en 1992 que  $g(X^{p,q}) \leq 4 \log_p q + \log_p 4 + 2$ , de sorte que la constante  $C = \frac{4}{3}$  du théorème 1 (ou de la proposition 2) est optimale.

**POUR EN SAVOIR PLUS**

**Biggs (N.-L.), Boshier (A.-G.),** Note on the girth of Ramanujan graphs, *J. Comb. Theory*, Ser. B **49**, n°2, 1990, 190-194.

**Davidoff (G.), Sarnak (P.), Valette (A.),** Elementary number theory, group theory and Ramanujan graphs, Cambridge Univ. Press, London Math. Soc. Student Texts 55, 2003.

**Dickson (L.-E.),** Arithmetic of quaternions, *Proc. London Math. Soc.*, (2) **20**, 1922, 225-232.

**Dickson (L.-E.),** *Linear groups with an exposition of the Galois field theory*, Dover Publications, New York, 1958.

**Erdős (P.), Sachs (H.),** Reguläre Graphen gegebener Tailleweite mit minimaler Knollenzahl, *Wiss. Z. Univ. Halle-Willenberg Math. Nat. R.*, **12**, 1963, 251-258.

**Lubotzky (A.), Phillips (R.), Sarnak (P.),** Ramanujan graphs, *Combinatorica*, **8**, 1988, 261-277.

**Margulis (G.-A.),** Explicit constructions of graphs without short cycles and low density codes, *Combinatorica*, **2**, 1982, 71-78.

**Margulis (G.-A.),** Explicit group-theoretical constructions of combinatorial schemes and their application to the design of expanders and concentrators, *J. Probl. Inf. Transm.*, **24**, n°1, 1988, 39-46.

**Weil (A.),** Sur les sommes de trois et quatre carrés (1974), Œuvres scientifiques Vol. III, Springer-Verlag, 1979.

# Transport optimal de mesure : coup de neuf pour un très vieux problème

**Bien connue depuis plusieurs siècles pour ses applications logistiques et économiques, la problématique du transport optimal de mesure connaît actuellement un renouveau spectaculaire à cause de ses liens insoupçonnés avec la mécanique des fluides, les équations aux dérivées partielles et d'autres domaines des mathématiques.**

On dit souvent que l'une des plus grandes satisfactions des mathématiciens consiste à établir des liens entre domaines *a priori* éloignés. L'histoire récente du transport optimal de mesure est à cet égard très représentative. Initié à la fin du XVIII<sup>e</sup> siècle par Monge, développé par Kantorovich au milieu du XX<sup>e</sup> siècle pour ses applications en économie, ce sujet a connu une renaissance spectaculaire dans les 15 dernières années, à partir des travaux de Brenier en mécanique des fluides. Les spécialistes actuels, peut-être frappés de délire monomaniaque voient maintenant du transport optimal partout : depuis les équations semi-géostrophiques en météorologie jusqu'aux problèmes isopérimétriques, en passant par les milieux granulaires, la physique statistique et les inégalités de Sobolev. Essayons de retracer quelques étapes de cette renaissance. Notons que, conformément à un phénomène assez courant, Brenier a « redécouvert » certains résultats déjà connus ; mais que cette redécouverte, loin d'être superflue, a apporté un nouvel éclairage au domaine qui, sans cela, n'aurait certainement pas acquis sa notoriété actuelle.

Pour comprendre le contexte dans lequel s'inscrivaient les travaux de Brenier, commençons par quelques rappels élémentaires de mécanique des fluides. L'**équation d'Euler incompressible** est l'une des équations les plus simples, les plus anciennes et les plus mystérieuses de toute la mécanique des fluides. Dans sa formulation dite Lagrangienne, elle peut se décrire comme suit. Soit  $\Omega$  un ouvert de  $\mathbb{R}^3$ , modélisant le récipient contenant le fluide, de volume normalisé à 1 ; on notera  $\lambda$  la mesure de Lebesgue restreinte à  $\Omega$ . L'état du fluide est modélisé par une application  $g(t, x)$ , où  $t$  est la variable de temps et  $x$  la variable d'espace ;  $g(t, x)$  représente la position au temps  $t$  d'une « particule » qui au temps 0 se serait trouvée au point  $x$ . Nous supposons que le flot est régulier,

au sens où pour tout  $t$ , l'application  $g(t, \cdot)$  est un difféomorphisme de  $\Omega$  sur  $\Omega$ . Pour traduire l'incompressibilité du fluide, on impose que  $g$  préserve la mesure de Lebesgue :  $g\#\lambda = \lambda$  (encadré 1). En d'autres termes, le volume occupé par un ensemble de particules donné ne varie pas au cours du temps. La fonction  $g(t, \cdot)$  appartient donc au groupe  $\text{SDiff}(\Omega)$  des *difféomorphismes de  $\Omega$  préservant la mesure de Lebesgue*.

Dans ce formalisme, l'équation d'Euler s'écrit

$$\frac{\partial^2 g}{\partial t^2}(t, x) = \nabla p(t, x), \quad (1)$$

où l'on note  $\nabla p$  le vecteur des dérivées partielles de la fonction scalaire  $p$  (« pression ») par rapport à  $x_1, x_2, x_3$ . Il ne faut pas spécifier d'équation sur  $p$  : cette marge de manœuvre est indispensable pour compenser la contrainte  $g \in \text{SDiff}(\Omega)$ . Une formulation plus connue de l'équation d'Euler, formellement équivalente à (1), porte sur le champ de vitesses  $u$  :  $\partial u / \partial t + (u \cdot \nabla)u + \nabla p = 0$ .

L'un des problèmes ouverts les plus célèbres de la théorie mathématique de la mécanique des fluides consiste à construire des solutions « raisonnables » de l'équation d'Euler. Sous certaines hypothèses de régularité, cela équivaut à construire des trajectoires qui *minimisent l'action, localement en temps* : pour tous temps  $t_0$  et  $t_1$  suffisamment proches, pour toute trajectoire  $m(t, \cdot)$  à valeurs dans  $\text{SDiff}(\Omega)$ , telle que  $m(t_0, \cdot) = g(t_0, \cdot)$  et  $m(t_1, \cdot) = g(t_1, \cdot)$ , on doit avoir

$$\int_{t_0}^{t_1} \left( \int_{\Omega} \left\| \frac{dg}{dt} \right\|^2 dx \right) dt \leq \int_{t_0}^{t_1} \left( \int_{\Omega} \left\| \frac{dm}{dt} \right\|^2 dx \right) dt. \quad (2)$$

En termes géométriques, le problème est de construire des *géodésiques* dans l'espace  $\text{SDiff}(\Omega)$ . Remarquons bien qu'il y a deux problèmes possibles :

---

– Cédric Villani, École normale supérieure de Lyon, UMPA, 46 allée d'Italie, 69364 Lyon cedex 07. [cvillani@umpa.ens-lyon.fr](mailto:cvillani@umpa.ens-lyon.fr)

**Encadré 1**

**MESURE IMAGE, MARGINALES**

Rappelons quelques notions élémentaires qui serviront tout au long de l'article.

Soit  $T$  une application,  $\mu$  et  $\nu$  deux mesures de probabilité.

On dit que  $\nu$  est la **mesure image** de  $\mu$  par  $T$ , ou que  $T$  **transporte** la mesure  $\mu$  sur la mesure  $\nu$ , et on note (par exemple)  $T\#\mu = \nu$ , si pour toute application mesurable positive (ou bornée)  $b$  on a

$$\int b(T(x)) d\mu(x) = \int b(y) d\nu(y). \quad (1)$$

Si  $T\#\mu = \mu$ , on dit que  $T$  **préserve la mesure**  $\mu$ . Par (1), on sait alors que  $\int b \circ T d\mu = \int b d\mu$  pour tout  $b \geq 0$ .

En particulier, pour tout  $p$ ,  $\|T\|_{L^p(d\mu)}^p$  est déterminé : c'est le moment d'ordre  $p$  de  $\mu$ .

Si  $\mu$  et  $\nu$  ont des densités respectives  $f$  et  $g$  par rapport à la mesure de Lebesgue, et si l'application  $T$  est injective et définit un changement de variable admissible (par exemple si c'est un  $C^1$  difféomorphisme), alors on établit aisément l'équation

$$f(x) = g(T(x)) |\det(DT(x))|,$$

où  $DT$  désigne l'application Jacobienne de  $T$ . C'est la formule classique du changement de variables !

Quand  $\mu$  et  $\nu$  sont définies sur le même espace, le transport de mesure peut s'exprimer en termes purement physiques : imaginons  $\mu$  et  $\nu$  comme les densités de répartition d'un grand nombre de particules. Ecrire  $T\#\mu = \nu$  revient à dire que si les particules sont au départ réparties selon la configuration  $\mu$  et que l'on transporte chaque particule de l'emplacement  $x$  à l'emplacement  $T(x)$ , alors les particules seront réparties, après transport, selon la configuration  $\nu$ .

Soit  $\pi$  une mesure de probabilité sur un espace produit  $X \times Y$ . On appelle **marginale** de  $\pi$  les mesures de probabilité  $\mu$  et  $\nu$  définies comme mesures images de  $\pi$  par les projections  $(x, y) \mapsto x$  et  $(x, y) \mapsto y$ . Prendre la marginale sur  $X$  revient à intégrer par rapport à  $y \in Y$ , et vice versa. De manière équivalente, pour toutes fonctions  $\varphi$  et  $\psi$  intégrables, on a

$$\int [\varphi(x) + \psi(y)] d\pi(x, y) = \int \varphi d\mu + \int \psi d\nu.$$

– soit on se donne la valeur de  $g(t, \cdot)$  en  $t = t_0$  et  $t = t_1$ , soit  $g_0$  et  $g_1$ , et on cherche à construire une solution (une trajectoire optimale) reliant  $g_0$  à  $g_1$ . En d'autres termes, on connaît l'état du fluide à deux instants donnés et on cherche à reconstituer la trajectoire entre ces deux instants ;

– soit on se donne la valeur de  $g(t, \cdot)$  en  $t = t_0$ , soit  $g_0$ , et sa dérivée (la vitesse initiale des particules),  $dg/dt|_{t=t_0}$ , et on cherche à prédire la trajectoire du fluide aux instants ultérieurs.

Les deux problèmes ne sont pas équivalents ; le premier est celui qui nous préoccupera. *A priori* plus simple que le second, il recèle cependant des surprises : par exemple, un résultat de Shnirelman implique qu'il n'existe pas toujours de trajectoire optimale.

**GEODÉSIIQUES APPROCHÉES**

Au milieu des années 80, pour tenter d'y voir plus clair, Brenier cherchait à construire des géodésiques approchées, par une procédure de discrétisation du temps. Considérons le cas extrêmement simplifié où il n'y a que trois temps :  $t_0$ ,  $t_1$ , et  $t_{1/2} = (t_0 + t_1)/2$ . On se donne  $g_0 = g(t_0, \cdot)$ ,  $g_1 = g(t_1, \cdot)$ , et on note  $\|m\|_{L^2} = \sqrt{\int m^2 dx}$ . Il est facile de s'apercevoir que la discrétisation du problème (2) consiste à rechercher

$g_{1/2} \in \text{SDiff}(\Omega)$  tel que pour tout  $m \in \text{SDiff}(\Omega)$ ,

$$\|g_1 - g_{1/2}\|_{L^2}^2 + \|g_{1/2} - g_0\|_{L^2}^2 \leq \|g_1 - m\|_{L^2}^2 + \|m - g_0\|_{L^2}^2. \quad (3)$$

Comme tous les éléments de  $\text{SDiff}(\Omega)$  ont la même norme  $L^2$  (encadré 1), l'équation (3) peut se réécrire : pour tout  $m \in \text{SDiff}(\Omega)$ ,

$$\|g_{1/2} - h\|_{L^2}^2 \leq \|m - h\|_{L^2}^2, \quad (4)$$

où  $h = (g_0 + g_1)/2$ . Autrement dit, le  $g_{1/2}$  que nous cherchons doit être la *projection orthogonale* du milieu  $h$  de  $g_0$  et  $g_1$ , sur le groupe  $\text{SDiff}(\Omega)$ , au sens de la norme  $L^2$ .

Comme le lecteur le vérifiera sans peine, le groupe  $\text{SDiff}(\Omega)$  n'est pas convexe ; par ailleurs, il n'est pas fermé au sens de la topologie  $L^2$ . La non-convexité empêche d'appliquer les théorèmes classiques de projection sur un convexe, mais ce n'est pas un problème fondamental très sérieux ; en revanche, on ne peut envisager de définir une projection sur un ensemble non fermé (que serait la projection d'un élément de  $\overline{\text{SDiff}(\Omega)} \setminus \text{SDiff}(\Omega)$  ?)... Il faut en conclure que le problème de minimisation (4) est en général *mal posé* : il n'admet pas toujours de solution pour un  $h$  général.



Pour contourner ce problème, on va appliquer une procédure classique du calcul des variations : la *relaxation*, qui consiste à remplacer l'espace trop restreint  $S\text{Diff}(\Omega)$  par son adhérence  $\overline{S\text{Diff}(\Omega)}$ . Ce dernier espace est constitué de toutes les applications  $s$  (pas nécessairement bijectives) préservant la mesure de Lebesgue ; on le notera  $S(\Omega)$ .

Il est possible de montrer par des théorèmes assez généraux que l'opération de projection sur  $S(\Omega)$  est « presque toujours » bien définie. Mais on peut mieux faire et donner une construction plus explicite. Soit  $\pi$  la mesure image sur  $\Omega \times \Omega$ , définie par  $\pi = (m \times h)\#\lambda$ . Par définition de la mesure image,

$$\begin{aligned} \|m - h\|_{L^2}^2 &= \int_{\Omega} |m - h|^2 \\ &= \int_{\Omega \times \Omega} |x - y|^2 d\pi(x, y). \end{aligned}$$

Par ailleurs, il est facile de vérifier que les marginales de  $\pi$  (encadré 1) sont la mesure de Lebesgue  $\mu = \lambda$  d'une part, et la mesure  $\nu = h\#\lambda$  d'autre part. Notre problème de minimisation peut maintenant être comparé au *problème plus général* qui consiste à minimiser la quantité

$$\int_{\Omega \times \Omega} |x - y|^2 d\pi(x, y)$$

parmi tous les  $\pi$ , mesures de probabilité sur l'espace produit  $\Omega \times \Omega$  dont les marginales sont  $\lambda$  et  $h\#\lambda$ . En développant le carré, on voit qu'il est équivalent de maximiser la quantité

$$\int_{\Omega \times \Omega} x \cdot y d\pi(x, y).$$

En termes probabilistes, nous cherchons à *maximiser les corrélations entre des variables aléatoires de lois respectives  $\mu$  et  $\nu$ , et dont la loi jointe serait l'inconnue  $\pi$ .*

Partis d'un problème de mécanique des fluides, nous avons abouti à un problème célèbre d'optimisation : le problème de **Monge-Kantorovich**. Sous sa version la plus générale, on peut l'énoncer ainsi : soient  $\mu$  et  $\nu$  deux mesures de probabilité sur des espaces respectifs  $X$  et  $Y$ , soit  $c : X \times Y \rightarrow \mathbb{R}_+$  une fonction, dite « fonction de coût » ; le problème consiste à minimiser la *fonctionnelle de coût*

$$\int_{X \times Y} c(x, y) d\pi(x, y)$$

parmi toutes les mesures  $\pi$  sur  $X \times Y$  admettant  $\mu$  et  $\nu$  pour marginales. Formulé pour la première fois sous cette forme par le célèbre économiste-mathématicien russe Leonid Kantorovich, ce problème avait été étudié dès 1780 par Gaspard Monge. L'existence d'un minimiseur est un exercice élémentaire d'analyse fonctionnelle,

qui ne nous apporte cependant guère d'informations sur le problème initial. Pour en savoir plus, on peut appliquer un célèbre principe de dualité dû à Kantorovich, et que nous appellerons le *principe du convoyeur* (encadré 2). Dans le cas qui nous intéresse, il aboutit à l'identité de type « minimax »

$$\sup_{\pi} \int x \cdot y d\pi(x, y) = \inf_{\varphi} \int \varphi d\mu + \int \varphi^* d\nu, \quad (5)$$

où l'infimum est pris sur toutes les paires  $(\varphi, \varphi^*)$  de fonctions convexes conjuguées :

$$\begin{cases} \varphi^*(y) = \sup_x (x \cdot y - \varphi(x)) \\ \varphi(x) = \sup_y (x \cdot y - \varphi^*(y)). \end{cases}$$

Le problème variationnel à droite de (5) ne semble guère plus simple que celui qui se trouve à gauche... Cependant, en termes de calcul des variations, il est considérablement plus agréable : sans perte de généralité, on peut fixer la valeur de  $\varphi$  en un point (cela ne change pas la valeur de l'infimum) ; or, les paires de fonctions convexes conjuguées  $(\varphi, \varphi^*)$ , définies sur un ouvert borné, ayant une valeur fixée en un point, forment un sous-ensemble *compact* de l'espace des fonctions continues sur cet ouvert. Le supremum est donc atteint dans le membre de droite de (5), par une paire de fonctions convexes.

Soit maintenant  $\pi$  une mesure optimale dans le problème de gauche de (5), et  $\varphi$  une fonction convexe optimale dans le problème de droite de (5) : en utilisant les propriétés de marginales, on peut écrire

$$\begin{aligned} \int_{\Omega \times \Omega} x \cdot y d\pi(x, y) &= \int_{\Omega} \varphi(x) d\mu(x) + \int_{\Omega} \varphi^*(y) d\nu(y) \\ &= \int_{\Omega \times \Omega} [\varphi(x) + \varphi^*(y)] d\pi(x, y), \end{aligned}$$

d'où

$$\int_{\Omega \times \Omega} [\varphi(x) + \varphi^*(y) - x \cdot y] d\pi(x, y) = 0.$$

Or, on a toujours  $\varphi(x) + \varphi^*(y) \geq x \cdot y$ , et donc nécessairement, pour  $\pi$  presque tous  $x$  et  $y$ ,

$$x \cdot y = \varphi(x) + \varphi^*(y).$$

Dans le langage de l'analyse convexe, on dit que  $y$  appartient au sous-différentiel  $\partial\varphi(x)$  de  $\varphi$  au point  $x$ . Pour peu que les mesures  $\mu$  et  $\nu$  soient absolument continues par rapport à la mesure de Lebesgue, on peut montrer que  $\partial\varphi(x) = \{\nabla\varphi(x)\}$  et en déduire que  $\nu = \nabla\varphi\#\mu$ , où l'on considère  $\nabla\varphi$  comme une application allant de  $\Omega$  dans

$\mathbb{R}^n$ . A partir de là, il est facile d'identifier notre projection orthogonale comme

$$s = \nabla\varphi^* \circ h = (\nabla\varphi)^{-1} \circ h. \quad (6)$$

Le résultat précédent peut sembler suspect : en composant les deux membres de (6) par  $\nabla\varphi$ , on obtient

$$h = \nabla\varphi \circ s : \quad (7)$$

l'application  $h$  est donc la composition de  $\nabla\varphi$  par une application préservant la mesure de Lebesgue – or, nous n'avons fait aucune hypothèse sur  $h$ , si ce n'est que  $h\#\lambda$  soit absolument continue... Il s'agit précisément du remarquable **théorème de factorisation polaire** de Brenier :

**Théorème 1.** Soit  $\Omega$  un ouvert borné de  $\mathbb{R}^d$  ( $d \geq 1$ ),  $\lambda$  la mesure de Lebesgue restreinte à  $\Omega$ , et  $h : \Omega \rightarrow \mathbb{R}^d$  un champ de vecteurs tel que la mesure image  $h\#\lambda$  soit absolument continue. Alors il existe une unique décomposition de  $h$  sous la forme

$$h = \nabla\varphi \circ s,$$

où  $\nabla\varphi$  est un gradient de fonction convexe sur  $\Omega$ , et  $s : \Omega \rightarrow \Omega$  est une application préservant la mesure de Lebesgue. En outre,  $s$  est l'unique projection orthogonale de  $h$  sur l'espace  $S(\Omega)$ .

Ce théorème présente de nombreux points communs avec d'autres théorèmes classiques : en particulier la factorisation polaire bien connue des matrices,  $M = SO$  ( $S$  symétrique,  $O$  orthogonale). Moins bien connue d'ailleurs, est la caractérisation du facteur  $O$  dans cette décomposition comme la projection orthogonale de  $M$  sur le groupe des matrices orthogonales ! Les géomètres pourront également reconnaître dans le théorème de Brenier une version non linéaire du théorème de décomposition de Hodge.

Laissons désormais de côté la mécanique des fluides et continuons à étudier le problème de minimisation de Monge-Kantorovich. Il existe en général de nombreuses manières de transporter des mesures l'une sur l'autre, et c'est un problème classique que de construire des transports « remarquables », en un certain sens. Or, nous venons de constater que deux mesures  $\mu$  et  $\nu$  sur  $\Omega$ , absolument continues, pouvaient être transportées l'une sur l'autre par un gradient de fonction convexe. Voici un énoncé un peu plus général :

**Théorème 2.** Soient  $d\mu(x) = f(x) dx$  et  $d\nu(y) = g(y) dy$  deux mesures de probabilité sur  $\mathbb{R}^d$ , absolument continues par rapport à la mesure de Lebesgue. Alors il existe un unique gradient de fonction convexe

## Encadré 2

### LE PRINCIPE DU CONVOYEUR (« SHIPPER »)

C'est une façon imagée d'exprimer la **dualité de Kantorovich**. Soit un mathématicien industriel devant organiser le convoi de sa production de charbon depuis les mines jusqu'aux usines. La production et la consommation de charbon sont représentées par des mesures positives, les quantités totales étant en adéquation (les mesures ont même masse). Le souci de notre mathématicien est de minimiser le coût dépensé en transport, soit  $\int c(x, y) d\pi(x, y)$ , où  $c(x, y)$  représente le coût du transport de  $x$  à  $y$ , et  $d\pi(x, y)$  la quantité élémentaire de charbon transportée du point  $x$  au point  $y$ . Les marginales de  $\pi$  sont fixées : ce sont respectivement les densités de charbon produit, et consommé ; nous sommes donc en présence d'un problème de Monge-Kantorovich. Un autre mathématicien se manifeste alors et suggère de lui sous-traiter le problème de transport : « Je me contenterai de te faire payer un prix à l'embarquement et un prix au débarquement ; ces prix varieront en fonction de l'emplacement, et je suis prêt à octroyer des compensations financières (prix négatifs) pour certains endroits. Tu y seras forcément gagnant, car la somme du prix d'embarquement et du prix de débarquement sera **toujours** inférieure ou égale au prix que tu paierais pour faire transporter la marchandise ! » Bien sûr, l'affaire est conclue.

Si l'on note  $\varphi(x)$  le prix à payer pour embarquer au point  $x$  et  $\psi(y)$  le prix à payer pour débarquer au point  $y$ , on voit que le convoyeur se fait payer

$$\int \varphi(x) d\mu(x) + \int \psi(y) d\nu(y). \quad (1)$$

Son problème est donc maintenant de fixer des prix  $\varphi$  et  $\psi$  de la manière la plus avantageuse, c'est-à-dire de façon à maximiser (1) tout en respectant la contrainte  $\varphi(x) + \psi(y) \leq c(x, y)$ , qui seule garantit que son offre est suffisamment attrayante pour qu'on lui laisse la charge de **tout** le transport.

Le **principe du convoyeur** (dualité de Kantorovich) assure que la somme d'argent (1) peut être aussi proche que l'on souhaite du coût optimal de Monge-Kantorovich. En termes mathématiques,

$$\inf_{\pi} \int c(x, y) d\pi(x, y) = \sup_{(\varphi, \psi)} \int \varphi d\mu + \int \psi d\nu,$$

où l'infimum à gauche est pris sur toutes les mesures  $\pi$  de marginales  $\mu$  et  $\nu$  et le supremum à droite est pris sur toutes les paires de fonctions de prix  $(\varphi, \psi)$  vérifiant l'inégalité  $\varphi(x) + \psi(y) \leq c(x, y)$  pour tous  $x$  et  $y$ .

(unique au sens de : déterminé  $f(x) dx$ -presque partout)  $\nabla\varphi$ , tel que

$$\nabla\varphi\#\mu = \nu.$$

De plus, si les seconds moments  $\int |x|^2 d\mu(x)$  et  $\int |y|^2 d\nu(y)$  sont finis, alors  $\varphi$  est l'unique minimiseur de la fonctionnelle de coût quadratique

$$\int |x - T(x)|^2 d\mu(x)$$

parmi toutes les applications  $T$  qui transportent  $\mu$  sur  $\nu$ .

Si  $f$ ,  $g$  et  $\varphi$  sont suffisamment régulières, alors on peut facilement en déduire (encadré 1) que  $\varphi$  est une solution de l'équation de Monge-Ampère

$$\det(D^2\varphi)(x) = \frac{f(x)}{g(\nabla\varphi(x))}.$$

L'étude de cette équation fort célèbre est considérée comme extrêmement ardue, du fait de son caractère « très non linéaire ». Le théorème 2 fournit donc une méthode, remarquablement simple et générale, pour construire des solutions faibles de cette équation. C'est un problème très délicat que de savoir si ces solutions faibles sont des solutions classiques... Dans une série d'articles difficiles, Caffarelli montre que si  $f$  et  $g$  sont strictement positives et de classe  $C^{k,\alpha}$  ( $k \in \mathbb{N}$ ,  $\alpha \in ]0, 1[$ ), au sens où leurs dérivées d'ordre  $k$  sont Hölder-continues d'exposant  $\alpha$ , alors  $\varphi$  est régulière, de classe  $C^{k+2,\alpha}$ . Ce résultat est bien sûr optimal dans sa catégorie.

### INTERPOLATION DE McCANN

Changeons radicalement de paysage physique. Au début des années 1990, McCann travaillait à démontrer l'unicité des formes d'équilibre de certains systèmes physiques (étoile, gaz en interaction...) dont l'état est

modélisé par une mesure de probabilité. Le problème mathématique se pose de la manière suivante : étant donnée telle ou telle fonctionnelle d'énergie  $F$ , peut-on démontrer qu'un minimiseur existe et qu'il est unique sous telle ou telle contrainte ? Le problème isopérimétrique et ses variantes (formes des cristaux, des gouttes d'eau, etc.) appartiennent à cette catégorie. Ces résultats d'unicité sont le plus souvent subordonnés à des propriétés de stricte convexité, selon un schéma de preuve très classique. En effet, si  $\mu$  et  $\nu$  sont deux minimiseurs, alors pour tout  $t \in [0, 1]$  on peut définir leur « interpolation linéaire »

$$\rho_t = (1 - t)\mu + t\nu. \quad (8)$$

Si  $F$  est strictement convexe, la fonction  $t \mapsto F(\rho_t)$  l'est également (sauf si  $\mu = \nu$ ), et présente un minimum strict pour un certain  $t \in ]0, 1[$  - ce qui contredit l'hypothèse de minimalité pour  $\mu$  et  $\nu$ . Bien évidemment, cette procédure classique ne s'appliquait pas aux exemples considérés par McCann (cela aurait été trop facile !!). Il eut cependant l'idée de substituer à l'interpolation (8) une autre recette, basée sur le transport optimal. Définissons donc, pour tout  $t$  (« temps ») compris entre 0 et 1,

$$\rho_t = [(1 - t)\text{Id} + t\nabla\varphi]\#\mu. \quad (9)$$

Bien sûr,  $\rho_0 = \mu$ ,  $\rho_1 = \nu$ .

Les deux exemples de la figure ci-dessous montreront combien cette procédure est qualitativement différente de la procédure plus classique d'interpolation linéaire. Dans chacun des deux cas envisagés, la densité de départ est représentée en vert, la densité d'arrivée en rouge, la densité interpolée en jaune. Les deux figures du haut considèrent une interpolation par transport de mesure (interpolation par déplacement), les deux figures du bas une interpolation linéaire. Noter que, dans les deux cas, non seulement la forme générale, mais aussi les supports des mesures interpolées sont différents.

Le théorème suivant, dû à McCann, illustre l'intérêt de cette procédure :

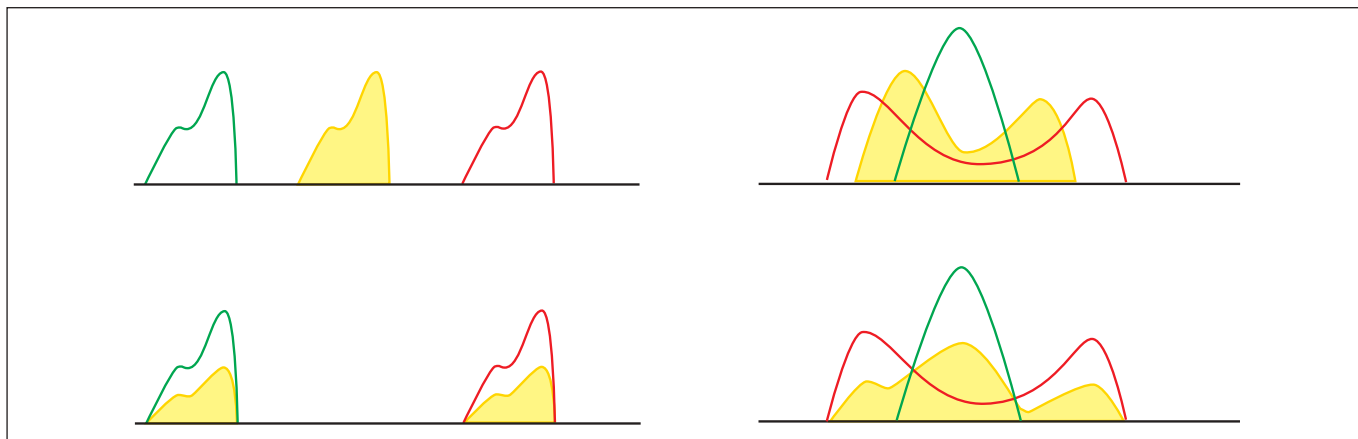


Figure - Différence entre l'interpolation « linéaire » et l'interpolation par transport.

**Théorème 3.** Soit  $W(z)$  une fonction convexe paire sur  $\mathbb{R}^d$  et soit  $\gamma \geq 1 - 1/d$ ,  $\gamma \neq 1$ . Alors la fonctionnelle

$$\rho \mapsto \frac{1}{\gamma - 1} \int \rho(x)^\gamma dx + \frac{1}{2} \int W(x - y) \rho(x) \rho(y) dx dy \quad (10)$$

est convexe le long de l'interpolation (9).

La formule (10) contient deux termes ; on peut penser au premier comme à un terme d'« énergie interne » et au second comme à un terme d'« énergie potentielle ». L'hypothèse de convexité du potentiel d'interaction  $W$  peut sembler mystérieuse, mais elle a trouvé des exemples d'application, de manière quelque peu surprenante, dans l'étude des milieux granulaires.

Divers résultats d'unicité résultent de ce théorème de « convexité par déplacement ». Des études plus poussées ont mis en évidence l'intérêt de ces notions dans l'étude de certaines équations issues de la mécanique statistique. Otto et ses collaborateurs ont ainsi montré qu'il existait un lien naturel entre l'équation de la chaleur, le transport optimal et la fonctionnelle d'entropie de Boltzmann,  $S(\rho) = -\int \rho \log \rho$ . Voici une formulation imagée de leur découverte. Soit  $\rho(t, x)$  la densité de particules diffusant librement, de sorte que  $\rho$  suit l'équation de la chaleur. Pour tout temps  $t \geq 0$ ,  $\rho(t) = \rho(t, \cdot)$  est une densité de probabilité. Entre deux instants infiniment proches  $t$  et  $t + dt$ , elle évolue de manière à **maximiser l'entropie**, tout en tenant compte d'une **pénalité** pour limiter les déplacements trop importants de particules : la quantité à maximiser est

$$S(\rho(t + dt)) - \frac{1}{2(dt)^2} T_2(\rho(t), \rho(t + dt)),$$

où  $T_2(\mu, \nu)$  désigne le coût de transport optimal entre  $\mu$  et  $\nu$ , pour le coût  $c(x, y) = |x - y|^2$ . Cet énoncé peut se traduire de manière compacte grâce au concept, bien connu en physique et en mathématiques, de **flot gradient**.

**APPLICATIONS A LA THÉORIE**

C'est une banalité que de dire que les mathématiques « pures » trouvent sans cesse des applications ; mais de manière également universelle en mathématiques, des concepts dont le développement a été motivé par des problèmes concrets trouvent des applications dans des ques-

tions d'apparence purement théorique. Le transport optimal n'échappe pas à la règle : il a trouvé des applications spectaculaires dans le domaine des inégalités fonctionnelles à caractère géométrique. Considérons ainsi la célèbre (pour les spécialistes !) inégalité de Young optimale,

$$\|f * g\|_{L^r(\mathbb{R}^d)} \leq \left( \frac{C_p C_q}{C_r} \right)^d \|f\|_{L^p(\mathbb{R}^d)} \|g\|_{L^q(\mathbb{R}^d)},$$

$C_p^2 = p^{1/p} / (p')^{1/p'}$ ,  $p' = p / (p - 1)$ , et  $1/p + 1/q = 1 + 1/r$ . Il en existe plusieurs démonstrations ; cependant, la plus spectaculaire est certainement celle qui a été mise au point par Barthe, reposant sur le transport optimal. Comme l'ont remarqué Cordero-Erausquin, Nazaret et l'auteur, il est également possible d'utiliser le transport de mesure pour démontrer avec peu d'efforts la non moins célèbre inégalité de Sobolev optimale,

$$\|f\|_{L^{p^*}(\mathbb{R}^d)} \leq S_d(p) \|\nabla f\|_{L^p(\mathbb{R}^d)},$$

où  $p^* = dp / (d - p)$ ,  $1 < p < d$ , et  $S_d(p)$  est la constante optimale. Bien sûr, le transport de mesure n'apparaît ici que comme un *outil*. Il en est de même pour le remarquable théorème suivant, dû à Caffarelli :

**Théorème 4.** Soient  $F, G, H, J, K$  des fonctions continues positives sur  $\mathbb{R}_+$ ,  $H$  et  $J$  étant croissantes, et soit  $k \in \mathbb{R}$ . Soit  $\rho$  une mesure de probabilité absolument continue, et soit  $\lambda(\rho)$  la plus grande constante  $\lambda$  admissible dans l'énoncé suivant : si  $\int K(h(x)) d\rho(x) = 0$ , alors

$$F\left(\int_{\mathbb{R}^d} G(|h(x)|) d\rho(x)\right) \leq \frac{1}{\lambda} H\left(\int_{\mathbb{R}^d} J(|\nabla h(x)|) d\rho(x)\right). \quad (11)$$

Soit maintenant  $\gamma$  la densité gaussienne standard :  $\gamma(x) = e^{-|x|^2} / (2\pi)^{d/2}$  ; et soit  $v$  une fonction convexe, normalisée de sorte que  $e^{-v}\gamma$  soit encore d'intégrale 1. Alors

$$\lambda(e^{-v}\gamma) \geq \lambda(\gamma).$$

En termes compacts : une inégalité fonctionnelle de la forme extrêmement générale (11) (qui inclut nombre d'inégalités de type isopérimétriques, trou spectral, etc.) ne peut être qu'améliorée par perturbation log concave d'une gaussienne. Encore une illustration des propriétés « miraculeuses » des fonctions gaussiennes...

**POUR EN SAVOIR PLUS**

**Ambrosio (L.), Brenier (Y.), Buttazzo (G.), Caffarelli (L.), Evans (L.-C.), Pratelli (A.) et Villani (C.)**, « Optimal transportation and applications », *Actes de l'école d'été CIME tenue à Martina Franca, septembre 2001*. Lecture Notes in Mathematics 1813, Springer-Verlag, 2002.

**Villani (C.)**, « Topics in optimal transportation », *Graduate Series in Mathematics*, American Mathematical Society, 2003.