ÉLOGES DES LAURÉATS DU CONGRÈS INTERNATIONAL DES MATHÉMATICIENS DE 2022

Traduits par Nicolas Bacaër

avec l'aide de Patrick Cégielski, Antoine Chambert-Loir, Aurélien Djament, Emeric Gioan, Rémy Mahfouf...

Éloges des lauréats du congrès international des mathématiciens de 2022

Traduits par Nicolas Bacaër

avec l'aide de Patrick Cégielski, Antoine Chambert-Loir, Aurélien Djament, Emeric Gioan, Rémy Mahfouf...

Textes sources :
www.mathunion.org ou dx.doi.org/10.4171/ICM2022
Beliaev (Dmitry) et Smirnov (Stanislav), *International Congress of Mathematicians 2022*, vol. I, Berlin, EMS Press, 2023.

Les textes ont été traduits automatiquement avec le logiciel DeepL puis relus et corrigés.

Pour la traduction :
Nicolas Bacaër
(Institut de recherche pour le développement, Bondy)
nicolas.bacaer@ird.fr
→ relecture des textes sur Maryna Viazovska et Nikolaï Andreïev

Patrick Cégielski
(Université Paris-XII, Fontainebleau)
→ relecture du texte sur Mark Braverman

Antoine Chambert-Loir
(Université Paris-Cité)
→ relecture du texte sur June Huh

Aurélien Djament
(Centre national de la recherche scientifique, Villetaneuse)
→ relecture du texte sur Barry Mazur

Emeric Gioan
(Centre national de la recherche scientifique, Montpellier)
→ relecture du texte sur June Huh

Rémy Mahfouf
(Université de Genève)
→ relecture du texte sur Hugo Duminil-Copin

Couverture : médaille Fields (Archimède et une citation en latin de Marcus Manilius « S'élever au-dessus de soi-même et conquérir le monde »).

Paris, Licence CC-BY-4.0
Dépôt légal : janvier 2025
ISBN : 979-10-426-5384-2

Introduction

> « Si celui dont j'étudie la langue ne respecte pas la mienne, parler sa langue cesse d'être un geste d'ouverture, il devient un acte d'allégeance et de soumission. »
>
> Amin Maalouf, *Les Identités meurtrières*

Les 5 940 pages des actes du congrès international des mathématiciens de 2022 ont été publiées en décembre 2023 par l'Union mathématique internationale et les presses de la Société mathématique européenne en accès libre au format PDF sous licence *Creative Commons* CC-BY-4.0 (« attribution »). Cela signifie que l'on peut utiliser librement ces textes à condition simplement de citer les noms des auteurs. Il est possible en particulier de les traduire en français. Certains fichiers sources en LaTeX sont par ailleurs disponibles sur le site `arXiv`, ce qui évite notamment d'avoir à retaper les formules mathématiques. On peut enfin utiliser un traducteur automatique tel que DeepL pour accélérer la traduction. Mais il faut évidemment relire pour s'assurer que les termes techniques ont été bien traduits, ce qui n'est pas toujours facile puisque ce congrès international rapporte les avancées de la recherche les plus récentes.

On trouvera dans ce recueil les traductions des éloges des lauréats de la médaille Fields, de la médaille de l'abaque, de la médaille Chern, du prix Gauss et du prix Līlāvatī. Ces éloges se trouvent dans le premier volume des actes (p. 26-162). Rappelons que certains textes de vulgarisation « grand public », qui figurent également dans ce premier volume (p. 548-570), ont déjà été traduits en français dans un autre recueil [1].

Des hyperliens renvoient vers des articles de Wikipédia à la première apparition d'un terme ou d'un nom dans le recueil. La liste de ces hyperliens figure en index. Les renvois à une partie d'un article et non à un article complet apparaissent en italique dans l'index.

Pour éviter d'avoir des dizaines de pages de bibliographie, on a limité les références au minimum nécessaire pour pouvoir les retrouver.

1. *Les lauréats des prix de l'Union mathématique internationale (1998-2022)*, hal.science/hal-04491414.

Dans un esprit un peu similaire à ce recueil, on rappelle l'existence des cinq volumes de *Leçons de mathématiques d'aujourd'hui*, publiés entre 2000 et 2019 par les éditions Cassini.

On remercie Jean-Louis Colliot-Thélène pour la relecture du texte sur James Maynard, Rupert Frank et Mathieu Lewin pour celle du texte sur Elliott Lieb, ainsi que Pierre McKenzie pour les précisions apportées pour la traduction de certains termes dans le texte sur Mark Braverman.

Nicolas Bacaër
Paris, décembre 2024

Sommaire

Les travaux d'Hugo Duminil-Copin (par Martin Hairer)

La dernière décennie a vu d'énormes progrès dans notre compréhension du comportement de nombreux modèles probabilistes au voisinage du « point critique ». Le 5 juillet 2022, Hugo Duminil-Copin a reçu la médaille Fields pour le rôle crucial qu'il a joué dans un bon nombre de ces développements. Dans ce court article de synthèse, nous tenterons de replacer ses travaux dans leur contexte et de présenter une petite sélection de ses résultats.

1 Introduction

Hugo Duminil-Copin s'est vu décerner la médaille Fields à Helsinki lors de la cérémonie d'ouverture du congrès international des mathématiciens virtuel de 2022. Dans cette courte note, je vais essayer de replacer son travail dans son contexte et de donner au lecteur un aperçu des raisons pour lesquelles les questions qu'il aborde sont non seulement très intéressantes d'un point de vue purement mathématique, mais contribuent également à approfondir notre compréhension de la nature à un niveau fondamental. Je commencerai tout d'abord par un avertissement. Hugo Duminil-Copin est un mathématicien avec une capacité extraordinaire à résoudre des problèmes. Bien que ses centres d'intérêt s'inscrivent clairement dans le domaine général de la théorie des probabilités et se focalisent en particulier sur les problèmes probabilistes qui se posent lors de l'étude de modèles microscopiques en physique statistique, je ne serai pas en mesure de rendre justice à l'ampleur de ses contributions. En outre, mon propre domaine d'expertise est quelque peu tangent à celui de Duminil-Copin, de sorte que cette note doit être considérée comme le point de vue d'une personne extérieure intéressée. En particulier, toute représentation erronée de ses résultats ou de ses techniques sera entièrement due à ma propre ignorance.

Au sens large, la physique statistique classique peut être considérée comme l'étude du comportement global des « grands » systèmes (de

Hairer (Martin), « The work of Hugo Duminil-Copin », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 26-49. DOI 10.4171/ICM2022/210

« taille » $N \gg 1$) qui sont constitués de nombreux « petits » sous-systèmes identiques qui interagissent les uns avec les autres. On indexe généralement les sous-systèmes par un ensemble discret Λ_N avec $\lim_{N\to\infty} |\Lambda_N| = \infty$ et l'on s'intéresse aux quantités qui sont stables lorsque $N \to \infty$. Dans de nombreux cas intéressants, on a $\Lambda_N \subset \Lambda$, où Λ est un sous-ensemble discret de l'espace euclidien (typiquement un réseau régulier). Ses éléments s'interprètent comme les positions physiques du sous-système correspondant. L'interaction entre les sous-systèmes peut alors dépendre de leurs positions. Dans la plupart des modèles, ils ne dépendent en fait que de leurs positions relatives, une notion qui se généralise très bien aux positions qui prennent des valeurs dans des espaces symétriques plus généraux.

Notons S l'espace d'état d'un seul de ces sous-systèmes. L'espace d'état du système complet est $\mathcal{S}_N \stackrel{\text{déf}}{=} S^{\Lambda_N}$. En *physique statistique à l'équilibre*, nous supposons en outre que S est muni d'une mesure de probabilité de « référence » μ (il faut penser à μ comme à une mesure de comptage normalisée si S est un ensemble fini, une mesure de volume normalisée s'il s'agit d'une variété compacte, etc.) et que notre système est décrit par une *fonction d'énergie* $H^{(N)} : \mathcal{S}_N \to \mathbb{R}$, qui comprend généralement une contribution de chaque sous-système, ainsi que des termes d'interaction supplémentaires. En toute généralité, on obtiendrait quelque chose comme

$$H^{(N)}(\sigma) = \sum_{A \subset \mathcal{S}_N} H_A(\sigma_A) \,, \tag{1}$$

où σ_A désigne la restriction de $\sigma \in S^{\Lambda_N}$ à S^A, et où la fonction H_A ne dépend généralement que de la « forme » du sous-ensemble A et vérifie donc les propriétés naturelles d'invariance par translation et éventuellement par réflexion ou rotation discrète. Dans de nombreux modèles classiques, les seuls termes non nuls dans (1) sont ceux avec $|A| \leqslant 2$.

Étant donné une telle fonction d'énergie, nous obtenons une mesure de probabilité $\mu_{\beta,N}$ sur $\mathcal{S}_N$ en posant

$$\mu_{\beta,N}(d\sigma) = Z_{\beta,N}^{-1} \exp\left(-\beta H^{(N)}(\sigma)\right) \prod_{u \in \Lambda_N} \mu(d\sigma_u) \,, \tag{2}$$

où $Z_{\beta,N}$ est choisi de telle sorte que $\mu_{\beta,N}(\mathcal{S}_N) = 1$. Physiquement, le paramètre $\beta > 0$ qui apparaît dans cette expression est l'inverse de la température du système. Dans une large mesure, la physique

statistique (à l'équilibre) est l'étude de $\mu_{\beta,N}$ lorsque $N \to \infty$, avec une attention particulière pour le comportement sous $\mu_{\beta,N}$ des observables qui prennent en compte un nombre « macroscopique » (de l'ordre de la taille de Λ_N) ou « mésoscopique » (qui tend vers l'infini lorsque $N \to \infty$ mais beaucoup plus petit que $|\Lambda_N|$) de composantes de σ.

1.1 La percolation de Bernoulli

L'exemple le plus simple est celui où $S = \{-1, 1\}$, $H_N = 0$ et $\mu(\{-1\}) = \mu(\{1\}) = \frac{1}{2}$. En ce qui concerne l'ensemble d'indices Λ_N, nous considérons le cas des éléments pairs d'une grande boîte dans $\mathbb{Z}^2$, à savoir $\Lambda_N = \{u \in \{-N, \dots, N\}^2 \,:\, u_1 + u_2 \text{ pair}\}$ [1].

L'un des types les plus simples d'observables « globaux » pour ce système est donné par le type suivant de statistique linéaire. Étant donné une fonction lisse $\varphi\colon [-1,1]^2 \to \mathbb{R}$, on définit $I_\varphi^N\colon \mathcal{S}_N \to \mathbb{R}$ par

$$I_\varphi^N(\sigma) = N^{-\alpha} \sum_{u \in \Lambda_N} \sigma_u \varphi\Big(u/N\Big) \,. \tag{3}$$

Notons que ceci est exhaustif : pour tout N fixé, si nous connaissons $I_\varphi^N(\sigma)$ pour toute fonction lisse φ, alors nous pouvons en principe retrouver l'argument σ lui-même. Une version du théorème central limite donne alors immédiatement le résultat suivant :

Théorème 1. *En fixant $\alpha = 1$, la loi jointe de $I_\varphi^N(\sigma)$ pour tout ensemble fini de fonctions test φ comme ci-dessus converge lorsque $N \to \infty$ vers la loi d'un ensemble de variables aléatoires gaussiennes centrées jointes I_φ telles que*

$$\mathbb{E} I_\varphi \, I_\psi = \frac{1}{2} \int_{[-1,1]^2} \varphi(x)\psi(x)\, dx \,.$$

Le facteur $\frac{1}{2}$ qui apparaît ici provient du fait que la densité locale de Λ_N dans $\mathbb{Z}^2$ est $\frac{1}{2}$.

Les propriétés de connectivité de σ, étudiées pour la première fois par Broadbent et Hammersley [12], sont un type d'observable globale beaucoup plus intéressant. Ces propriétés sont cependant beaucoup plus difficiles à analyser. Même si le modèle que nous venons de décrire semble à première vue quelque peu trivial, la plupart des résultats à

1. La raison pour laquelle nous faisons ce choix étrange au lieu de prendre simplement tous les éléments de $\{-N, \dots, N\}^2$ deviendra bientôt claire.

son sujet nous conduisent déjà directement dans les mathématiques du XXI^e siècle. Afin de décrire ce que nous entendons par « connectivité » dans ce contexte, au lieu d'interpréter les éléments $u \in \Lambda_N$ comme des points dans $\mathbb{Z}^2$, nous les interprétons comme les arêtes les plus proches d'un sous-réseau approprié de $\mathbb{Z}^2$ en associant à u l'unique arête e_u de $\mathbb{Z}_{\text{pair}} \times \mathbb{Z}_{\text{impair}}$ avec comme milieu u. Nous noterons par ailleurs e_u^* l'arête de $\mathbb{Z}_{\text{impair}} \times \mathbb{Z}_{\text{pair}}$ avec comme milieu u. En d'autres termes, nous définissons

$$e_u = \begin{cases} (u_\downarrow, u_\uparrow) & \text{si } u_1 \text{ est pair,} \\ (u_\leftarrow, u_\rightarrow) & \text{si } u_1 \text{ est impair,} \end{cases}$$

$$e_u^* = \begin{cases} (u_\leftarrow, u_\rightarrow) & \text{si } u_1 \text{ est pair,} \\ (u_\downarrow, u_\uparrow) & \text{si } u_1 \text{ est impair.} \end{cases}$$

Ici, étant donné $u = (u_1, u_2) \in \mathbb{Z}^2$, on écrit $u_\leftarrow = (u_1 - 1, u_2)$, etc. Les extrémités de ces arêtes appartiennent bien aux sous-réseaux indiqués de $\mathbb{Z}^2$ puisque $u_1 + u_2$ est pair, donc soit u_1 et u_2 sont pairs, soit ils sont impairs.

Étant donné une configuration $\sigma \in \mathcal{S}_N$, nous interprétons les arêtes e_u avec $\sigma_u = -1$ comme « ouvertes » et les dessinons en noir, tandis que les autres arêtes sont considérées comme « fermées » et sont dessinées en gris clair. On obtient ainsi une image comme celle présentée à gauche dans la figure 1. On peut alors se demander par exemple quelle est la probabilité p_N qu'il soit possible d'aller du bord gauche du graphe gris clair au bord droit (le « bord » est ici constitué des extrémités des arêtes pendantes) en ne traversant que des arêtes noires. Il s'avère que cette probabilité prend des valeurs non triviales même pour de grandes valeurs de N. En fait, elle est indépendante de N comme le montre le résultat classique suivant (voir par exemple [36, lemme 11.21]).

Théorème 2. *On a* $p_N = \frac{1}{2}$ *pour tout* N.

Démonstration. L'astuce consiste à observer qu'étant donné une configuration $\sigma \in \mathcal{S}_N$, si nous dessinons la configuration duale $\sigma^* \in \mathcal{S}_N$ définie par $\sigma_u^* = -\sigma_u$ en coloriant (disons en gris) les arêtes e_u^* avec $\sigma_u^* = -1$, alors nous obtenons un dessin ayant la propriété que les arêtes grises ne touchent jamais les arêtes noires. Par conséquent, il est possible de traverser le carré de gauche à droite en ne passant que par des arêtes noires si et seulement s'il n'est pas possible de le traverser de haut en bas en ne passant que par des arêtes grises (voir fig. 1). D'autre part, la loi de l'ensemble des arêtes grises est la même que celle de l'ensemble

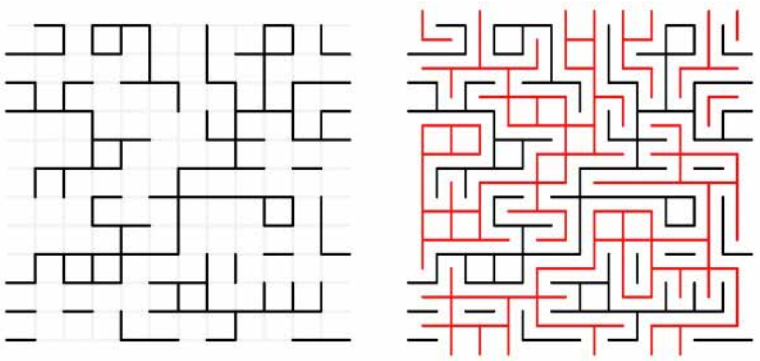


FIG. 1 – *À gauche, on dessine une configuration de percolation typique pour* N = 11. *À droite, la même configuration est dessinée avec sa configuration duale en gris.*

des arêtes noires, mais tournée de 90°, de sorte que nous devons avoir $p_N = 1 - p_N$ comme annoncé. □

Remarque 1. Si, au lieu de choisir des arêtes ouvertes avec une probabilité $\frac{1}{2}$, nous les choisissons ouvertes avec une probabilité p, alors nous avons $p_N \to 1$ pour $p > \frac{1}{2}$ et $p_N \to 0$ pour $p < \frac{1}{2}$. Il s'agit d'un exemple de *transition de phase* : un changement abrupt dans le comportement de certaines observables globales lorsqu'un paramètre du modèle varie de manière continue. Dans cet exemple particulier, nous avons pu déterminer la *valeur critique* $p_c = \frac{1}{2}$ explicitement en exploitant une dualité exacte.

Il est également possible d'obtenir un large ensemble d'observables globales intéressantes en prenant une forme $\mathcal{U} \subset [-1,1]^2$ difféomorphe à un carré et en considérant l'événement analogue $A_{\mathcal{U}}^{(N)} \subset \mathcal{S}_N$ en demandant s'il est possible de relier les bords gauche et droit de $N\mathcal{U}$ (sans jamais quitter $N\mathcal{U}$) par un chemin qui suit uniquement les arêtes ouvertes d'une configuration donnée $\sigma \in \mathcal{S}_N$. Encore une fois, la connaissance de ces événements est une statistique exhaustive pour toute valeur fixe donnée de N. On sait en outre que, pour tout nombre fini de ces formes $\{\mathcal{U}_i\}_{i\in I}$ (pour I un ensemble d'indices fini), les variables aléatoires $\{[A_{\mathcal{U}_i}^{(N)}]\}_{i\in I}$ convergent en loi vers une limite non dégénérée $\{[A_{\mathcal{U}_i}]\}_{i\in I}$ lorsque $N \to \infty$ [56] (la notation [A] désigne ici la fonction

indicatrice d'un événement A). Un fait étonnant est que cette limite d'échelle est invariante par transformation conforme : si $\varphi\colon \mathrm{D} \to \mathrm{D}'$ est une application conforme entre deux domaines lisses simplement connexes D et $\mathrm{D}' \subset \mathbf{C}$ tels que $[-1,1]^2 \subset \mathrm{D}$ et $\mathcal{V}_i \stackrel{\text{déf}}{=} \varphi(\mathcal{U}_i) \subset [-1,1]^2$, alors la loi jointe des variables aléatoires $\{[\mathrm{A}_{\mathcal{V}_i}]\}_{i\in\mathrm{I}}$ est *la même* que celle de $\{[\mathrm{A}_{\mathcal{U}_i}]\}_{i\in\mathrm{I}}$.

Cette invariance conforme s'avère être une caractéristique cruciale des limites d'échelle de nombreux modèles de physique statistique à l'équilibre en deux dimensions. Elle établit un lien avec la théorie conforme des champs, qui peut être considérée à un niveau purement mathématique comme l'étude des représentations irréductibles des algèbres de Virasoro. En particulier, elle suggère fortement que les comportements possibles à grande échelle que l'on peut observer pour les modèles à l'équilibre à deux dimensions se présentent sous la forme d'une famille à un paramètre de « classes d'universalité » paramétrées par la charge centrale de la théorie conforme des champs correspondante. Dans le cas de la percolation, il s'avère que cette charge centrale est donnée par $c = 0$.

1.2 Le modèle d'Ising

Le modèle suivant « le plus simple » en physique statistique dans la catégorie des modèles à l'équilibre décrits ci-dessus est le modèle d'Ising [41, 43] (voir également l'article de synthèse [16] qui donne un compte rendu plus détaillé des divers développements suscités par ce modèle). Dans ce cas, l'ensemble d'indices est donné par $\Lambda_\mathrm{N} = \{-\mathrm{N}, \dots, \mathrm{N}\}^d$ avec $d \geqslant 1$, la mesure de référence μ et l'espace d'état local S sont les mêmes que ci-dessus, mais $\mathrm{H}_\mathrm{A} = 0$ sauf si $\mathrm{A} = \{u, v\}$ avec u et $v \in \mathbb{Z}^d$ tels que $|u - v| = 1$, auquel cas on pose $\mathrm{H}_\mathrm{A}(\sigma) = -\sigma_u\sigma_v$. Cette fois, le modèle a une dépendance non triviale par rapport au paramètre β dans (2), qui joue un rôle quelque peu similaire au paramètre p qui figurait dans la remarque 1.

À un niveau très qualitatif, la situation est similaire à ce qui se passe dans le cas de la percolation : pour toute dimension $d \geqslant 2$, il existe une valeur critique β_c qui dépend de la dimension et qui délimite deux régimes différents. À « haute température », c'est-à-dire pour $\beta < \beta_c$, l'*aimantation spontanée*, à savoir la quantité aléatoire $\mathrm{N}^{-d} \sum_{i\in\Lambda_\mathrm{N}} \sigma_i$ converge en probabilité vers 0 lorsque $\mathrm{N} \to \infty$. Pour $\beta > \beta_c$, elle converge en probabilité vers une variable aléatoire limite qui peut prendre exactement deux valeurs possibles $\pm h_\beta \neq 0$ avec des probabilités

égales. La valeur exacte de β_c n'est connue qu'en dimension 2 [50] où elle est égale à

$$\beta_c = \log \sqrt{1 + \sqrt{2}}.$$

Il n'y a pas de transition de phase du tout en dimension 1 : l'aimantation spontanée disparaît toujours, donc en un certain sens $\beta_c = +\infty$ dans ce cas.

Il est à nouveau possible de se poser les mêmes questions que dans le cas de la percolation de Bernoulli. Cette fois cependant, même l'analogue du théorème 1, qui était une conséquence essentiellement triviale du théorème central limite (ou du moins d'une version de celui-ci), est déjà fortement non trivial. Une série récente de travaux [13,14] a montré que si l'on choisit $\beta = \beta_c$ et $\alpha = 15/8$ dans l'expression (3) en dimension $d = 2$, celle-ci converge en loi vers des variables aléatoires limites non triviales, conjointement pour tout nombre fixé de fonctions test. Mais les lois limites ne sont pas gaussiennes (elles présentent en fait un comportement avec une queue qui décroît encore plus rapidement). Notons que l'exposant α est étroitement lié au comportement de $\mathbb{E}_c\sigma_u\sigma_v$ (où $\mathbb{E}_c$ désigne l'espérance par rapport à la mesure de Gibbs (2) pour la valeur critique de la température inverse β) puisqu'on trouve, en supposant que $\mathbb{E}_c\sigma_u\sigma_v \approx |u - v|^{-\delta}$,

$$\begin{aligned}\mathbb{E}_c\Big(\mathrm{I}^{\mathrm{N}}_{\varphi}(\sigma)\Big)^2 &= \mathrm{N}^{-2\alpha} \sum_{u,v} \varphi(u/\mathrm{N})\varphi(v/\mathrm{N})\mathbb{E}_c\sigma_u\sigma_v \\ &\lesssim \mathrm{N}^{-2\alpha} \sum_{u,v} |u - v|^{-\delta} \approx \mathrm{N}^{2d-(\delta\wedge d)-2\alpha}\,,\end{aligned}$$

de sorte que l'on s'attend à la relation $\alpha = d - (\delta \wedge d)/2$, qui conduit (correctement) à la prédiction $\delta = \frac{1}{4}$. Ceci et un certain nombre d'autres propriétés du modèle d'Ising au point critique permettent de l'associer à la théorie conforme des champs avec une charge centrale $c = \frac{1}{2}$.

La situation en dimensions supérieures est cependant beaucoup moins claire. Pour $d \geqslant 5$, [1,2,29] ont montré que l'exposant d'échelle correct à utiliser dans (3) lorsque $\beta = \beta_c$ est $\alpha = 1 + \frac{d}{2}$ et que la limite est un champ libre gaussien, à savoir la loi gaussienne avec une fonction de corrélation donnée par la fonction de Green du laplacien (avec la condition aux limites de Neumann sur le carré). En dimension $d = 3$, on ne sait pratiquement rien de rigoureux sur le modèle d'Ising critique, pas même la valeur de ses exposants critiques, bien que de nombreux progrès aient été réalisés à un niveau non rigoureux avec le

développement du « *bootstrap* conforme » [23, 24]. En ce qui concerne le cas $d = 4$, il n'était pas clair jusqu'à très récemment si le modèle d'Ising au point critique devait être « trivial » (c'est-à-dire décrit par des lois gaussiennes) ou non. Cette question a finalement été résolue par Aizenman et Duminil-Copin dans leur article [3], dans lequel ils montrent que toute limite d'une sous-suite pour les expressions de la forme (3) lorsque $N \to \infty$ (et $\beta \to \beta_c$) est nécessairement gaussienne.

En fait, certains des résultats mentionnés ci-dessus sont démontrés pour le « modèle Φ^4 sur réseau » qui est le modèle à l'équilibre avec $S = \mathbb{R}$,

$$H_{\{u\}}(\sigma) = V(\sigma_u) \stackrel{\text{déf}}{=} \sigma_u^4 - \alpha\sigma_u^2 , \quad H_{\{u,v\}}(\sigma) = \tfrac{1}{2}(\sigma_u - \sigma_v)^2 ,$$

à condition que u et v soient des voisins directs et avec α qui est un paramètre supplémentaire. Bien que ce modèle semble à première vue très différent du modèle d'Ising, nous pouvons voir qu'il s'agit en fait d'une généralisation de celui-ci : si la constante α est grande, alors le potentiel V possède deux puits très profonds avec des minima situés à $\pm\sqrt{\alpha}$, ce qui a pour effet d'imposer que $\sigma_u \approx \pm\sqrt{\alpha}$ avec une forte probabilité. La contribution principale vient alors du terme croisé dans le développement du carré qui est le même que pour le modèle d'Ising. Ces considérations nous amènent à penser que, puisque ces modèles présentent des corrélations à longue portée à la température critique (dans le sens où la corrélation $\mathbb{E}\sigma_x\sigma_y$ décroît lentement avec $|x - y|$ comme nous l'avons déjà souligné), ce qui devrait en outre conduire à une certaine forme d'auto-moyennisation, le modèle d'Ising et le modèle Φ^4 présentent le même comportement à leurs températures critiques respectives.

1.3 Une vue d'ensemble

La vue d'ensemble qui devrait maintenant se dégager de notre discussion peut être résumée ainsi :

1. De nombreux systèmes locaux à l'équilibre parmi les plus simples présentent une transition de phase, c'est-à-dire qu'il existe une valeur critique β_c à laquelle le comportement qualitatif à grande échelle du système change brusquement. Un système peut en général dépendre de paramètres supplémentaires, auquel cas on peut observer un *diagramme de phase* plus compliqué avec plusieurs régions dans l'espace des paramètres où le comportement global du système affiche un comportement qualitativement

différent. Dans tous les cas, on s'attend à ce que la phase « haute température » (avec β petit) se comporte de telle manière que des régions bien séparées soient pratiquement indépendantes.

2. En dimension 2, beaucoup de ces systèmes semblent présenter une forme d'invariance conforme au point critique, même si aucune symétrie de rotation n'est intégrée *a priori* dans leur description. Lorsque cela se produit, le lien avec les théories conformes des champs en dimension 2 (et les objets probabilistes associés comme l'évolution de Schramm-Loewner [55], l'évolution de Loewner quantique [45], etc.) fournit un mécanisme extrêmement puissant pour prédire leur comportement et dans un certain nombre de cas pour le démontrer rigoureusement.

3. L'univers des modèles locaux en physique statistique peut être subdivisé en grandes classes de modèles qui présentent un comportement commun à grande échelle au point critique. Ces classes sont appelées « classes d'universalité ». Dans le cas des modèles à l'équilibre en dimension 2, on s'attend à ce qu'elles se présentent sous forme de familles paramétrées par un nombre réel, la charge centrale. Pour certaines valeurs de la charge centrale, on s'attend à avoir plusieurs « sous-classes », mais nous ne discuterons pas de ce genre de subtilité ici.

4. Bien que l'on s'attende toujours à une invariance conforme au point critique dans les dimensions supérieures, cette symétrie y est beaucoup plus contraignante et semble donc offrir un peu moins de renseignements [2]. On s'attend également à ce que la situation y soit plus rigide qu'en dimension 2, avec moins de classes d'universalité. Il est possible qu'il n'y ait qu'une famille discrète.

5. Les modèles qui ont des variantes « évidentes » dans toutes les dimensions ont généralement une dimension critique au-dessus de laquelle leur comportement au point critique est « trivial » : il présente un comportement gaussien, typiquement avec une fonction de corrélation donnée par la fonction de Green du laplacien. Cette dimension critique est 4 dans le cas de la classe d'universalité du modèle d'Ising et 6 dans le cas de la percolation de Bernoulli.

2. Voir toutefois la percée récente réalisée dans l'approximation des exposants critiques du modèle d'Ising en dimension 3 à l'aide du « *bootstrap* conforme » [23,24] déjà mentionné plus haut.

Une branche importante de la théorie moderne des probabilités vise à donner à cette image générale une base mathématique rigoureuse. Le reste de cet article est consacré à un bref aperçu des nombreuses contributions d'Hugo Duminil-Copin à ce vaste programme. Cela ne représente bien sûr qu'une infime partie de son travail et en ignore des pans entiers. En présentant non pas une longue liste de résultats qu'il a démontrés et de conjectures qu'il a résolues, mais plutôt un aperçu de la stratégie de démonstration pour quelques résultats choisis, j'espère pouvoir transmettre l'une des caractéristiques de l'œuvre de Duminil-Copin, à savoir qu'il a le don de trouver la bonne façon d'aborder un problème, une façon souvent négligée. Dans de nombreux cas, cela n'apporte que de petites fissures dans l'armure du problème, qui requièrent encore une grande habileté technique pour être ouvertes. Mais dans certains cas, cela aboutit à des démonstrations étonnamment simples mais ingénieuses. Quoi qu'il en soit, je suis impatient d'en apprendre davantage grâce aux idées de Duminil-Copin dans les années à venir.

2 (Dis)continuité des transitions de phase

Une question très naturelle dans ce domaine est de savoir si l'on peut prendre la limite $N \to \infty$ dans l'équation (2). À ce stade, on remarque que la définition de $H^{(N)}$ donnée dans (1) n'est pas nécessairement la plus naturelle puisqu'elle restreint la somme sur les amas A qui sont contraints de se situer *entièrement* dans S_N. Une autre possibilité qui semble tout aussi naturelle consisterait à restreindre la somme sur les amas qui coupent simplement S_N, mais en spécifiant une « condition aux limites » fixe $\bar{\sigma} \in S^{\Lambda}$ qui serait utilisée pour calculer les valeurs de H_A avec A qui coupe à la fois Λ_N et $\Lambda \setminus \Lambda_N$: nous interprétons σ_A dans (1) comme $\sigma_{A,x} = \sigma_x$ pour $x \in A \cap \Lambda_N$ et $\sigma_{A,x} = \bar{\sigma}_x$ sinon.

Dans de nombreux exemples intéressants (y compris dans le cas du modèle d'Ising mais *pas* dans le cas de la percolation), la mesure $\mu_\beta = \lim_{N\to\infty} \mu_{\beta,N}$ est bien définie (c'est-à-dire indépendante du choix des conditions aux limites) pour $\beta < \beta_c$ alors que l'on peut obtenir plusieurs limites différentes dans le cas $\beta > \beta_c$. La figure 2 montre des exemples typiques sous μ_β pour le modèle d'Ising avec $\bar{\sigma} \equiv 1$. Dans le cas où $\beta > \beta_c$, la configuration consiste en une « mer » de spins qui prennent la valeur dominante +1 (en gris foncé) avec de petits « îlots » de spins qui prennent la valeur −1 (en gris clair). Si nous avions fixé $\bar{\sigma} \equiv -1$, nous aurions obtenu un exemple au comportement opposé, ce

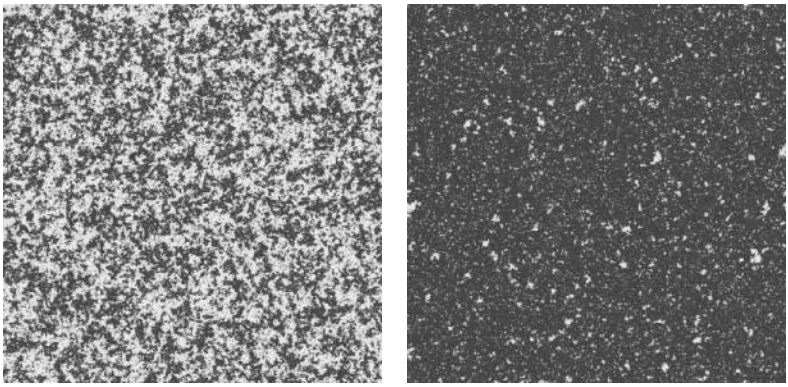


FIG. 2 – *Configurations typiques du modèle d'Ising pour $\beta < \beta_c$ (à gauche) et $\beta > \beta_c$ (à droite).*

qui illustre la non-unicité de la mesure à volume infini μ_β dans ce cas. Dans le cas $\beta < \beta_c$ en revanche, chacune des deux valeurs possibles du spin est à peu près également représentée et la mesure est symétrique par rapport à la substitution $1 \leftrightarrow -1$, ce qui illustre l'unicité de μ_β. C'est en fait un théorème dans le cas du modèle d'Ising : pour $\beta > \beta_c$, il existe exactement deux mesures à volume infini invariantes par translation $\mu_\beta^\pm$ qui correspondent aux conditions aux limites $\bar{\sigma} \equiv \pm 1$ et toute limite de sous-suite des $\mu_{\beta,\mathrm{N}}$ pour toute condition aux limites suffisamment homogène lorsque $\mathrm{N} \to \infty$ est une combinaison convexe de μ_β^+ et μ_β^-.

Ceci soulève la question de l'unicité de μ_β à $\beta = \beta_c$. Si c'est le cas, on dit que la transition de phase est *continue*, sinon on dit qu'elle est *discontinue*. Cette terminologie vient du fait que la continuité en ce sens est équivalente à la continuité des applications $\beta \mapsto \mu_\beta^\pm$ à $\beta = \beta_c$. On sait depuis longtemps [5, 60] que la transition de phase du modèle d'Ising est continue en dimension $d = 1$ et 2 ainsi qu'en dimension $d \geqslant 4$. La raison pour laquelle les dimensions 1 et 2 sont généralement beaucoup mieux comprises est que le modèle d'Ising est « résoluble » dans ces dimensions : on peut obtenir des expressions explicites pour l'espérance d'un grand nombre d'observables sous $\mu_{\beta,\mathrm{N}}$ (cette solution est simple pour $d = 1$ [41] où il n'y a pas de transition de phase, mais ce fut une avancée majeure lorsque Onsager obtint la solution exacte pour $d = 2$ [50]). La dimension $d = 4$ est en revanche la « dimension critique

supérieure » au-delà de laquelle le modèle est censé être « trivial », c'est-à-dire décrit par des variables aléatoires gaussiennes dans la limite d'échelle, ce qui permet d'utiliser un certain nombre de techniques puissantes, notamment le *développement en lacets* [39,54].

Il reste donc le cas $d = 3$, qui est bien sûr le plus intéressant physiquement puisque le modèle d'Ising est un modèle-jouet du ferromagnétisme et que ses dimensions représentent les dimensions spatiales habituelles. Des considérations heuristiques suggèrent que la transition de phase y est également continue, ce qui est cohérent avec les expériences physiques, en supposant que le modèle d'Ising appartienne à la même classe d'universalité que celle d'un véritable aimant physique. Dans l'article [4], Duminil-Copin et ses collaborateurs ont donné la première démonstration rigoureuse que c'est bien le cas. La démonstration repose sur l'introduction de la quantité

$$\mathrm{M}(\beta) = \inf_{\mathrm{B}\subset\mathbb{Z}^3} \frac{1}{|\mathrm{B}|^2} \sum_{x,y\in\mathrm{B}} \int \sigma_x\sigma_y \, \mu_\beta^0(d\sigma) \, ,$$

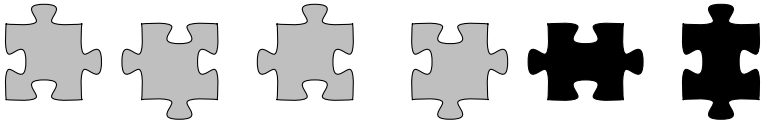
où μ_β^0 désigne la limite de volume infini obtenue en utilisant des conditions « libres », ainsi que sur trois étapes principales. Tout d'abord, ils s'appuient sur des résultats de [30,31] pour affirmer que la transformée de Fourier de $x \mapsto \int \sigma_0\sigma_x, \mu_\beta^0(d\sigma)$ se trouve dans L^1 lorsque $\beta = \beta_c$, ce qui implique que $\mathrm{M}(\beta_c) = 0$. Ensuite, et c'est l'étape principale, ils montrent que le fait d'avoir $\mathrm{M}(\beta) = 0$ implique qu'un certain modèle de percolation avec des corrélations à longue portée construit à partir du modèle d'Ising n'admet pas d'amas infini. Enfin, ils utilisent une variante du « lemme d'inversion » [35] pour montrer que la quantité $\int \sigma_0\sigma_x \, \mu_\beta^+(d\sigma) - \int \sigma_0\sigma_x \, \mu_\beta^0(d\sigma)$ est majorée par une fonction explicite multipliée par la probabilité que l'origine appartienne à un amas infini dans le modèle ci-dessus, et doit donc s'annuler en $\beta = \beta_c$. Une fois cela connu, il est facile de montrer que l'aimantation spontanée du modèle d'Ising au point critique doit s'annuler (on a $\in \sigma_0 \, \mu_{\beta_c}^+(d\sigma) = 0$), ce qui à son tour donne l'énoncé d'unicité souhaité.

Pour illustrer le fait que la continuité de la transition de phase, quelle que soit la dimension, est une propriété non triviale qui n'est pas nécessairement attendue en général, un bon exemple est celui du modèle de Potts [53]. Ce modèle est défini de manière similaire au modèle d'Ising, mais cette fois l'espace d'état local S est donné par $\mathrm{S} = \{1, \ldots, q\}$ pour un entier $q \geqslant 2$, doté à nouveau de la mesure de comptage normalisée comme mesure de référence. Comme pour le

modèle d'Ising, on pose $H_A = 0$ sauf si $A = \{u, v\}$ avec u et $v \in \mathbb{Z}^d$ tels que $|u - v| = 1$, auquel cas on pose $H_A(\sigma) = \mathbf{1}_{\sigma_u = \sigma_v}$. Pour $q = 2$, ce modèle est équivalent au modèle d'Ising puisque leurs fonctionnelles d'énergie ne diffèrent que par une constante. Remarquons également qu'il existe un modèle essentiellement équivalent appelé « modèle d'amas aléatoire » ou parfois « modèle FK », d'après Fortuin et Kasteleyn qui l'ont introduit dans [28]. Dans ce modèle, on considère directement des partitions de $\mathbb{Z}^d$ en « amas » connexes, que l'on peut considérer comme les composantes reliées par des arêtes des ensembles $\{u : \sigma_u = i\}$ pour $i \in S$ et une configuration donnée σ du modèle de Potts. Ce modèle a également un sens pour des valeurs non entières de $q \geqslant 1$. Dans le cas $q = 1$, le modèle FK se réduit en fait à une percolation de Bernoulli régulière. Voir (12) ci-dessous pour une définition plus précise de ce modèle.

Baxter a conjecturé dans les années soixante-dix [8, 9] que le modèle de Potts sur $\mathbb{Z}^2$ présentait une transition de phase continue si et seulement si $q \leqslant 4$. Les deux articles [17, 21] de Duminil-Copin et de ses collaborateurs fournissent des démonstrations des deux sens de cette conjecture. Par souci de brièveté, nous ne commenterons pas les démonstrations en détail, mais nous remarquons que la démonstration de la continuité de la transition de phase pour $q \leqslant 4$ est presque complètement disjointe de celle pour le modèle d'Ising en dimension 3. Une étape importante consiste à nouveau à montrer que le modèle au point critique avec des conditions aux limites égales à un élément fixe de S n'admet pas d'amas infini. Cependant, la démonstration de ce fait (qui exploite une forme d'holomorphie discrète de certaines observables astucieusement choisies) et la démonstration de son équivalence avec l'unicité de la mesure à volume infini au point critique sont complètement différentes. En fait, elles montrent l'équivalence d'une liste de cinq propriétés bien distinctes qui sont d'un intérêt indépendant pour l'étude du modèle de Potts au point critique.

En ce qui concerne la démonstration de la *dis*continuité lorsque $q > 4$, l'outil principal est une relation étroite, d'abord découverte par Temperley et Lieb [59] dans un contexte restreint, puis par Baxter et ses collaborateurs [10] dans un contexte plus général, entre le modèle FK sur $\mathbb{Z}^2$ et le « modèle à six sommets ». Les configurations de ce dernier modèle peuvent être visualisées comme des puzzles où l'on assigne à chaque sommet de $\mathbb{Z}^2$ (ou à un sous-ensemble de celui-ci) l'une des six pièces (orientées)



et où l'on applique la contrainte d'admissibilité selon laquelle les pièces s'emboîtent parfaitement. On postule en outre que la probabilité de voir une configuration admissible donnée est proportionnelle à $c^{\#p}$, où $\#p$ représente le nombre de pièces noires dans la configuration et c est une constante fixée. La relation entre le modèle à six sommets et le modèle FK critique vaut pour le choix particulier

$$c = \sqrt{2 + \sqrt{q}}.$$

L'avantage de cette relation est que le modèle à six sommets est « résoluble » dans un certain sens en utilisant le formalisme de la matrice de transfert. On n'est pas pour autant sorti d'affaire, car les matrices de transfert V_N impliquées sont très grandes : elles agissent sur un espace vectoriel de dimension 2^N, mais sont diagonales par blocs, chaque bloc $V_N^{[n]}$ agissant sur un sous-espace de dimension $\binom{n}{N}$. Chacun de ces blocs est irréductible avec des éléments strictement positifs et admet donc un vecteur propre de Perron-Frobenius. Le principal résultat technique de [21] est un résultat asymptotique très précis pour les valeurs propres de Perron-Frobenius de $V_N^{[N/2-r]}$ pour r fixé lorsque $N \to \infty$. Il est intéressant de noter que les auteurs sont capables de démontrer que les rapports entre ces valeurs propres convergent vers des limites finies (et explicites, au moins sous forme de séries convergentes explicites) lorsque $N \to \infty$ et que les valeurs propres elles-mêmes divergent exponentiellement en fonction de N avec un exposant connu, mais le comportement commun d'ordre inférieur de cette divergence n'est pas connu. Ce résultat asymptotique est cependant suffisant pour obtenir un bon contrôle sur la fonction de partition du modèle à six sommets et pour l'exploiter afin d'obtenir une expression explicite pour l'inverse de la longueur de corrélation du modèle de Potts critique avec des conditions aux limites libres lorsque $q > 4$. La finitude de cette expression permet enfin de déduire la discontinuité de la transition de phase.

Pour conclure cette section, j'aimerais mentionner le magnifique article [20] qui, bien qu'il ne traite pas tout à fait de la question de la continuité de la transition de phase, a une saveur proche. La question est celle du caractère « abrupt » de la transition de phase, qui se formule dans ce cas particulier comme la question de savoir s'il est vrai que la

mesure μ_β a des corrélations qui décroissent exponentiellement (dans le sens où la covariance entre $f(\sigma_0)$ et $f(\sigma_x)$ décroît exponentiellement vite lorsque $|x| \to \infty$ pour toute fonction $f : S \to \mathbb{R}$ « suffisamment bonne ») pour *tout* $\beta < \beta_c$ et pas seulement pour des valeurs suffisamment petites où un argument de perturbation au voisinage de $\beta = 0$ (où $f(\sigma_0)$ et $f(\sigma_x)$ sont indépendants sous μ_0 dès que $x \neq 0$) peut s'appliquer. Une difficulté avec ce type d'énoncé est que l'on ne connaît généralement pas d'expression explicite pour β_c : dans le cas du modèle FK sur le réseau carré, on peut obtenir une pareille expression par un argument de dualité [11], mais on n'en connaît pas pour des situations plus générales. Le résultat principal de [20] est que la transition de phase du modèle FK sur *tout* graphe infini sommet-transitif est abrupte.

L'outil principal de leur démonstration est une généralisation nouvelle et de grande portée de l'inégalité OSSS [49]. Le contexte est celui des variables aléatoires croissantes $f : \{0,1\}^E \to [0,1]$ (pour un ensemble fini E et pour l'ordre partiel naturel coordonnée par coordonnée sur $\{0,1\}^E$), où $\{0,1\}^E$ est en outre doté d'une mesure de probabilité $\mathbb{P}$ qui est elle-même *monotone* : pour tout $F \subset E$ et tout $e \in E \setminus F$, les probabilités conditionnelles $\mathbb{P}(w_e = 1 \,|\, \mathcal{F}_F)$ sont des fonctions croissantes (ici, $\mathcal{F}_F$ désigne la tribu engendrée par les applications $w \mapsto w_e$ pour $e \in F$). On considère alors *tout* algorithme qui révèle une par une les valeurs d'une entrée $w \in \{0,1\}^E$ de telle sorte que la coordonnée à révéler ensuite dépende de manière déterministe de l'information glanée à partir de ce qui a été révélé jusqu'à ce point. En particulier, la première coordonnée à révéler est toujours la même puisqu'aucune information n'a encore été obtenue à ce stade. L'algorithme s'arrête lorsque les valeurs révélées sont suffisantes pour déterminer la valeur de $f(w)$, ce qui donne un ensemble aléatoire $\hat{E} \subset E$ de valeurs révélées. Le résultat de [20] est alors que l'on a l'inégalité

$$\mathrm{Var}(f) \leqslant \sum_{e \in E} \mathbb{P}(e \in \hat{E}) \, \mathrm{Cov}(f, w_e) \,, \tag{4}$$

qui semble formellement identique au résultat de [49], mais l'hypothèse y était que la mesure $\mathbb{P}$ est simplement la mesure uniforme. Comme cette dernière est clairement monotone — elle est telle que $\mathbb{P}(w_e = 1 \,|\, \mathcal{F}_F)$ soit constante — les résultats de [49] en découlent comme un cas particulier.

En utilisant ce résultat, [20] obtient alors la dichotomie suivante qui donne le résultat souhaité relatif au caractère abrupt.

Théorème 3. *Soit* G *un graphe transitif et soit* $\mathbb{P}_{\beta,n}$ *la mesure FK sur la boule* Λ_n *de rayon n dans* G. *Il existe alors* $\beta_c \in \mathbb{R}$ *tel que, pour tout* $\beta < \beta_c$, *il existe* $c_\beta > 0$ *tel que* $\mathbb{P}_{\beta,n}(0 \leftrightarrow \partial\Lambda_n) \lesssim e^{-c_\beta n}$, *uniformément par rapport à n. Pour* $\beta > \beta_c$ *d'autre part, il existe* $c > 0$ *tel que* $\mathbb{P}_{\beta,n}(0 \leftrightarrow \partial\Lambda_n) \geqslant c \min\{1, \beta - \beta_c\}$.

Une fois l'inégalité (4) connue, la démonstration est étonnamment simple et repose sur deux ingrédients. Premièrement, on peut montrer que les mesures $\mathbb{P}_{\beta,n}$ et la fonction $\mathbf{1}_{0\leftrightarrow\partial\Lambda_n}$ vérifient les hypothèses de l'inégalité (4). En fixant $\theta_n(\beta) = \mathbb{P}_{\beta,n}(0 \leftrightarrow \partial\Lambda_n)$, un choix astucieux d'algorithme de recherche pour l'amas (potentiel) reliant l'origine 0 à $\partial\Lambda_n$ permet alors de montrer que l'on a l'inégalité

$$\theta_n'(\beta) \gtrsim \sum_{e\in \mathrm{E}} \mathrm{Cov}_\beta(\mathbf{1}_{0\leftrightarrow\partial\Lambda_n}, w_e) \geqslant \frac{n}{8\Sigma_n(\beta)}\theta_n(\beta)(1-\theta_n(\beta)) \,, \qquad (5)$$

où $\Sigma_n = \sum_{k=0}^{n-1} \theta_n$. Le fait que la première inégalité soit valable est connu et peut être vérifié de manière élémentaire. Le second fait est que *toute* suite de fonctions $\beta \mapsto \theta_n(\beta)$ qui vérifie une inégalité différentielle de la forme (5) vérifie nécessairement une dichotomie du type qui apparaît dans l'énoncé du théorème 3. Comme nous ne nous intéressons pas au régime où θ_n est grand, nous pouvons réécrire (5) sous la forme $\theta_n' \geqslant \frac{cn}{\Sigma_n}\theta_n$. Le fait que les fonctions θ_n doivent alors respecter une telle dichotomie est assez clair : si β est tel qu'elles convergent vers une limite non nulle θ, alors $\Sigma_n/n \sim \theta$ et on doit avoir $\theta' \geqslant c$. Si en revanche elles convergent vers 0 sur tout un intervalle $[a, b]$, alors cette convergence doit avoir lieu suffisamment rapidement pour que $\Sigma_n/n \gg \theta_n$ (car sinon l'argument précédent s'appliquerait). Puisque $\Sigma_n/n \sim \theta_n$ pour $\theta_n \sim n^{-\alpha}$ dès que $\alpha < 1$, il est alors plausible que pour tout $c < b$ on ait $\theta_n \ll n^{-1/2}$ (par exemple), ce qui implique $\theta_n' \gtrsim \sqrt{n}\theta_n$ et donc $\theta_n \lesssim e^{-\sqrt{n}(c-\beta)}$ pour $\beta < c$. Cela montre que la suite de fonctions Σ_n est bornée pour $\beta < c$, ce qui conduit à $\theta_n' \gtrsim n\theta_n$ et donc à une borne exponentiellement petite (par rapport à n), comme indiqué.

3 Trivialité de Φ_4^4

Depuis les travaux novateurs d'Osterwalder et Schrader [51, 52], on sait que la construction d'une théorie quantique des champs (bosonique) qui vérifie les axiomes de Wightman est équivalente au moins dans certains cas à la construction d'une mesure de probabilité sur l'espace des distributions qui vérifie un certain nombre de propriétés naturelles.

L'un des sommets de ce champ de recherche a été la construction dans les années soixante-dix des mesures Φ^4_2 et Φ^4_3 [22, 25, 27, 33, 34, 47, 48, 57], qui correspondent au cas le plus simple d'une théorie d'interaction en deux ou trois dimensions d'espace-temps avec un seul type de boson.

À un niveau heuristique, la mesure Φ^4_d est la mesure $\mu^{(d)}$ sur l'espace des distributions de Schwartz $\mathcal{S}'(\mathbb{R}^d)$ (ou sur le tore de dimension d) donnée par

$$Z^{-1} \exp\left(-\frac{1}{2}\int \left(|\nabla\Phi(x)|^2 - C\Phi^2(x) + \Phi^4(x)\right) dx\right) d\Phi \,,$$

où « $d\Phi$ » désigne la mesure de Lebesgue en dimension infinie sur $\mathcal{S}'(\mathbb{R}^d)$. Cette expression est bien sûr problématique à plusieurs niveaux : la mesure de Lebesgue en dimension infinie n'existe pas, les distributions ne peuvent pas être élevées au carré, etc. S'il n'y avait que le terme $|\nabla\Phi|^2$, on pourrait raisonnablement interpréter cette expression comme la mesure gaussienne μ_0 avec un opérateur de covariance donné par la fonction de Green du laplacien, qui est une mesure de probabilité bien définie (à l'exception de détails techniques liés au mode constant qui peuvent être facilement corrigés). La mesure μ_0 est appelée « champ libre gaussien », car elle correspond à une théorie quantique des champs dans laquelle les particules sont libres, c'est-à-dire qu'elles n'interagissent pas du tout entre elles.

Ceci suggère qu'une interprétation plus fine de la mesure Φ^4_d pourrait être donnée par

$$\mu^{(d)}(d\Phi) = Z^{-1} \exp\left(-\frac{1}{2}\int \Phi^4(x)\, dx\right) \mu_0(d\Phi) \,. \tag{6}$$

Ceci est encore mal défini puisque le champ libre gaussien a comme support des distributions plutôt que des fonctions pour toute dimension $d \geqslant 2$. Cependant, en posant $\Phi_\varepsilon = \rho_\varepsilon \star \Phi$, la *puissance de Wick*

$$:\Phi^4: = \lim_{\varepsilon\to 0}\left(\Phi^4_\varepsilon - 3\Phi^2_\varepsilon \mathbb{E}\Phi^2_\varepsilon\right) \tag{7}$$

s'avère être une distribution de Schwartz aléatoire bien définie (c'est-à-dire que la limite existe et elle est indépendante du choix de ρ_ε) en dimension $d < 4$. En dimension 2, Nelson a montré dans [47] que le facteur de Radon-Nikodym qui apparaît dans (6) avec Φ^4 remplacé par $:\Phi^4:$ donne une variable aléatoire intégrable, ce qui conduit à une définition de $\mu^{(2)}$. En particulier, la mesure Φ^4_2 est équivalente au champ

libre gaussien. En dimension 3, il s'avère que ce n'est pas le cas, mais il est encore possible de montrer que la mesure $\mu^{(3)}(d\Phi)$ égale à

$$\lim_{\varepsilon\to 0} Z_\varepsilon^{-1} \exp\left(-\frac{1}{2}\int \Phi_\varepsilon^4(x) - C_\varepsilon \Phi_\varepsilon^2(x)\,dx\right)\mu_0(d\Phi) \tag{8}$$

est bien définie pour un choix approprié de la constante C_ε qui diffère du choix $3\mathbb{E}\Phi_\varepsilon^2 \sim \varepsilon^{-1}$ suggéré par (7) par un terme qui diverge logarithmiquement. Une autre construction de cette mesure a été récemment obtenue par des techniques complètement différentes dans [37, 38, 46].

Cette discussion soulève la question de savoir ce qui se passe pour $d \geqslant 4$ et en particulier lorsque $d = 4$ qui est le cas physiquement le plus intéressant du point de vue de la théorie quantique des champs (rappelons que la dimension correspond ici à l'espace-temps). En ce qui concerne le cas $d > 4$, Aizenman et Fröhlich ont déjà montré dans les années quatre-vingt [1, 2, 29] que pratiquement toute définition « raisonnable » de la mesure Φ_d^4 coïncide en fait avec le champ libre gaussien. Il reste le cas $d = 4$ qui a toujours été considéré comme le cas le plus difficile, car il est « critique » dans le sens où, au moins à un niveau formel, les termes Φ^4 et $|\nabla\Phi|^2$ ont le même ordre de grandeur dans le sens suivant. En écrivant $\mathcal{S}_\lambda$ pour la transformation $(\mathcal{S}_\lambda F)(x) = F(\lambda x)$, le champ libre gaussien possède la propriété d'autosimilarité

$$\mathcal{S}_\lambda \Psi \overset{\text{loi}}{=} \lambda^{\frac{2-d}{2}} \Psi$$

pour Ψ tiré de μ_0. En supposant que Ψ se comporte comme une fonction (même s'il s'agit en réalité d'une distribution aléatoire), on en déduit que

$$\mathcal{S}_\lambda |\nabla\Psi|^2 = \lambda^{-2} |\nabla \mathcal{S}_\lambda \Psi|^2 \overset{\text{loi}}{=} \lambda^{-d} |\nabla\Psi|^2\,,$$

$$\mathcal{S}_\lambda(\Psi^4) = (\mathcal{S}_\lambda \Psi)^4 \overset{\text{loi}}{=} \lambda^{4-2d}\Psi^4\,.$$

Ces exposants sont en effet égaux si et seulement si $d = 4$. Un calcul heuristique suggère en fait qu'à l'ordre suivant, le terme $|\nabla\Psi|^2$ domine le terme Ψ^4 à grande échelle. Des variantes de cette observation ont été rendues rigoureuses dans un certain nombre de travaux [26, 32, 40], y compris tout récemment dans une série impressionnante de travaux de Bauerschmidt-Brydges-Slade (voir [6, 7] et les références qui s'y trouvent).

Une façon de formuler l'un de leurs principaux résultats est le cadre donné dans notre introduction avec $S = \mathbb{R}$, μ étant la mesure de

Lebesgue, $H_{\{x\}}(\varphi) = \frac{g}{4}\varphi_x^4 + \frac{\nu}{2}\varphi_x^2$, $H_{\{x,y\}}(\varphi) = |\varphi_x - \varphi_y|^2$ lorsque x et y sont des sites voisins du réseau $\mathbb{Z}^4$, et $H_A = 0$ sinon. Ce modèle se comporte d'une manière très similaire au modèle d'Ising, en lequel il dégénère dans le régime $g \to \infty$ et $\nu = -g$. On considère traditionnellement le modèle Φ^4 avec $\beta = 1$, puisqu'on peut toujours se ramener à ce cas en ajustant g et ν, et éventuellement en changeant l'échelle des φ_x par un facteur. On considère généralement que g est fixé. C'est donc le paramètre ν qui est ajustable et joue le rôle d'une « température » dans ce modèle. Tout comme pour le modèle d'Ising, il présente une transition de phase à une certaine valeur $\nu_c \in \mathbb{R}$: pour $\nu > \nu_c$, il existe une unique mesure en volume infini qui est symétrique par rapport à la transformation $\varphi \mapsto -\varphi$. Pour $\nu < \nu_c$ en revanche, on trouve deux mesures en volume infini distinctes (ainsi que leurs combinaisons convexes) selon les conditions aux limites que l'on choisit.

Un état $\varphi \in S^{\Lambda_N}$ avec $\Lambda_N = \{-N, \dots, N\}^4$ est vu comme une distribution $\iota\varphi$ sur le tore (de dimension 2) en posant, pour toute fonction test lisse $f : \mathbf{T}^4 \to \mathbb{R}$,

$$\big(\iota\varphi\big)(f) = \sum_{x \in \Lambda_N} \sigma_N \varphi_x f(x/N)$$

pour une suite de valeurs σ_N choisies de telle sorte que $\mathbb{E}\Big((\iota\varphi)(1)^2\Big) = 1$. [6] montre alors que si g est suffisamment petit et si ν est choisi de manière appropriée (proche mais pas tout à fait égal à la valeur critique ν_c), alors $\iota\varphi$ converge vers un champ libre gaussien massif, à savoir le champ gaussien dont la covariance est donnée par $(m^2 - \Delta)^{-1}$ pour un certain $m \in \mathbb{R}$ (qui dépend de la manière particulière avec laquelle ν est réglé pour approcher ν_c quand $N \to \infty$).

Bien que ce résultat suggère fortement qu'il n'existe pas de mesure Φ_4^4 non triviale, il n'exclut pas la possibilité d'avoir une limite d'échelle non triviale pour le champ discret que nous venons de décrire au point (ou près du point) critique lorsque la constante g est suffisamment grande (en d'autres termes « avec un couplage fort »). La technique de démonstration de [6] a consisté à mettre en œuvre une version rigoureuse de la « technique du groupe de renormalisation », qui repose sur une analyse subtile du comportement de l'application de renormalisation au voisinage du point fixe donné par le champ libre gaussien. Cette technique est malheureusement perturbative par nature et n'a donc que peu d'espoir de pouvoir traiter des g arbitraires. Dans un travail récent [3] cependant, Aizenman et Duminil-Copin ont finalement réussi à montrer le résultat suivant.

Théorème 4. *Pour toute manière d'ajuster $g = g_N$ et $\nu = \nu_N$ quand $N \to \infty$ de sorte que $\nu_N \geqslant \nu_{c,N}$, pour tout $M_N \to \infty$ avec $1 \ll M_N \ll N$ et pour toute fonction test lisse à support compact f, la loi de $\xi_N^f = \sum_{x \in \Lambda_N} \varphi_x f(x/M_N)$, normalisée de sorte que sa variance soit égale à un, converge vers une loi normale.*

Remarque 2. La condition $\nu_N \geqslant \nu_{c,N}$ peut en fait être légèrement relaxée, mais pas trop. En effet, dans le régime des « basses températures » et avec des conditions aux limites libres (ou périodiques), on s'attendrait à ce que la loi de ξ_N^f converge vers une variable aléatoire de Bernoulli plutôt que vers une gaussienne.

À un niveau supérieur, la principale raison pour laquelle [3] peut traiter des couplages arbitraires est que l'on peut considérer que leur cadre est plus proche de la « perturbation autour de $g = \infty$ » qu'autour de $g = 0$. Dans le cadre de l'introduction, ils commencent par considérer le modèle d'Ising tel qu'il y est décrit, c'est-à-dire avec $\mu = \frac{1}{2}(\delta_1 + \delta_{-1})$, mais ils étendent ensuite leur classe de modèles pour permettre à chaque site de représenter un ensemble de spins avec des interactions ferromagnétiques arbitraires au sein d'un site, au lieu d'un seul spin. Ceci a pour effet de remplacer μ par toute mesure qui peut être obtenue comme la loi de $\delta \sum_{i=1}^{K} s_i$ pour un certain $\delta > 0$ et $K \in \mathbb{N}$, et où les $s_i \in \{-1, 1\}$ sont des variables aléatoires dont la loi jointe est proportionnelle à $\exp(-\sum_{ij} a_{ij} s_i s_j)$ avec des coefficients a_{ij} arbitraires mais *strictement positifs*. Comme on l'a déjà montré dans les années soixante-dix [58, théorème 1], toutes les mesures de probabilité sur $\mathbb{R}$ du type $Z^{-1} \exp(cx^2 - gx^4)\, dx$ peuvent s'obtenir comme limites de telles mesures, de sorte que le modèle Φ_4^4 discret peut être considéré comme une limite des modèles à blocs de spins.

Rappelons que pour montrer qu'un ensemble $\{X_a\}_{a \in A}$ de variables aléatoires à valeurs réelles a une loi jointe gaussienne, il suffit de montrer que tous les cumulants joints d'ordre quatre $\mathbb{E}_c\{X_{a_1}, \dots, X_{a_4}\}$ avec $a_i \in A$ s'annulent. Il n'est donc pas surprenant que les cumulants d'ordre quatre des variables de spin jouent un rôle important dans toute démonstration du caractère gaussien des modèles de type Ising. En dimension $d \geqslant 5$, la démonstration dans [2] s'appuie sur deux observations très importantes. Premièrement, en notant $C(x, y) = \mathbb{E}\big(\sigma_x \sigma_y\big)$ la fonction de corrélation de spin, on montre que pour toute température et toute interaction

ferromagnétique, on a l'inégalité

$$\left|\mathbb{E}_c\{\sigma_{x_1},\dots,\sigma_{x_4}\}\right| \leqslant 2\sum_{y\in\mathbb{Z}^d} \mathrm{C}(x_1,y)\cdots\mathrm{C}(x_4,y)\ . \tag{9}$$

On observe alors que la fonction C est bornée *à la température critique* par

$$\mathrm{C}(x,y) \lesssim |x-y|^{2-d}\ . \tag{10}$$

Considérons maintenant quatre fonctions test lisses à support compact f_i et posons

$$\mathrm{X}_i = \sum_{x\in\mathbb{Z}^d} \sigma_x f_i(x/\mathrm{M})\ .$$

En particulier, la somme s'étend sur $O(\mathrm{M}^d)$ sites. Si l'on suppose que (10) est optimal, on s'attend à avoir $\mathbb{E}\mathrm{X}_i^2 \approx \mathrm{M}^{d+2}$, de sorte que la normalisation « correcte » pour que les X_i aient une variance égale à 1 devrait être $\xi_i = \mathrm{M}^{-\frac{d+2}{2}}\mathrm{X}_i$. D'autre part, en combinant la borne sur la covariance avec la borne sur le cumulant d'ordre quatre, un argument de comptage de puissance montre que $\mathbb{E}_c\{\xi_1,\dots,\xi_4\} \lesssim \mathrm{M}^{-2(d+2)}\mathrm{M}^{d+8} = \mathrm{M}^{4-d}$, qui converge effectivement vers 0 quand $\mathrm{M}\to\infty$ pour $d>4$, ce qui montre que les ξ_i ont une loi jointe gaussienne à la limite.

Il est clair que ce calcul ne nous permet pas de conclure quoi que ce soit lorsque $d=4$. La principale contribution de [3] est de montrer que l'inégalité (9) peut en fait être améliorée en une inégalité du type

$$\left|\mathbb{E}_c\{\sigma_{x_1},\dots,\sigma_{x_4}\}\right| \lesssim \frac{\sum_{y\in\mathbb{Z}^d}\mathrm{C}(x_1,y)\cdots\mathrm{C}(x_4,y)}{\left(\sum_{|x|\leqslant\mathrm{M}}\mathrm{C}(0,x)^2\right)^c} \tag{11}$$

pour un certain $c>0$ (éventuellement très petit). On suppose ici que les x_i sont tous à des distances au moins M les uns des autres.

Remarque 3. Si l'on pense que la borne (10) représente le comportement correct de C au point critique, alors le dénominateur qui apparaît dans l'inégalité (11) est d'ordre $(\log \mathrm{M})^c$ en dimension 4. Ceci n'est cependant pas connu et n'est pas non plus utilisé par [3], que ce soit pour obtenir l'inégalité (11) ou pour en déduire le théorème 4.

La démonstration de l'inégalité (11) repose sur la représentation en « courants aléatoires » du modèle d'Ising dans laquelle l'espace de configuration est constitué de « courants », à savoir d'applications $\mathbf{n}\colon \mathrm{E}\to\mathbb{N}$ où E désigne l'ensemble des paires de plus proches voisins

(non orientées) dans notre réseau. La mesure d'Ising conduit alors naturellement à un poids w sur les courants défini par $w(\mathbf{n}) = \prod_{e \in \mathrm{E}} \frac{\beta^{\mathbf{n}(e)}}{\mathbf{n}(e)!}$ ainsi qu'à la notion de « source » d'un courant définie par

$$\partial \mathbf{n} \stackrel{\text{déf}}{=} \left\{ x \,:\, \sum_{e \ni x} \mathbf{n}(e) \text{ est impair} \right\} .$$

Le lien entre les courants et le modèle d'Ising est donné la formule suivante : étant donné un ensemble fini $\mathrm{A} \subset \mathbb{Z}^d$, on a

$$\mathbb{E} \prod_{a \in \mathrm{A}} \sigma_a = \frac{\sum_{\mathbf{n} \,:\, \partial \mathbf{n} = \mathrm{A}} w(\mathbf{n})}{\sum_{\mathbf{n} \,:\, \partial \mathbf{n} = \emptyset} w(\mathbf{n})} .$$

Une notion naturelle est alors celle de « courant aléatoire de source A » pour lequel la probabilité de voir un courant donné $\mathbf{n}$ est non nulle seulement lorsque $\partial \mathbf{n} = \mathrm{A}$, auquel cas elle est proportionnelle à $w(\mathbf{n})$. Lorsque $\mathrm{A} = \{x, y\}$, un courant $\mathbf{n}$ avec une source A peut être interprété (mais pas de manière unique !) comme la mesure d'occupation d'un ensemble de boucles dans $\mathbb{Z}^d$, ainsi qu'un chemin sans auto-intersection joignant x et y. En particulier, la restriction de $\mathbf{n}$ à l'ensemble de boucles qui sont reliées (directement ou indirectement par d'autres boucles) au chemin joignant x et y peut être considérée comme la mesure d'occupation d'un seul chemin aléatoire joignant x à y.

L'inégalité (11) peut alors être reformulée en termes de propriétés d'intersection de ces chemins aléatoires. D'un point de vue heuristique, il est très utile de considérer ces trajectoires aléatoires comme de simples trajectoires de marche aléatoire. Notons que la dimension 4 est critique pour la question de savoir si les traces de deux trajectoires se croisent ou non : pour $d < 4$, les trajectoires de deux marches aléatoires indépendantes avec deux points de départ quelconques se croisent presque sûrement. En revanche, pour $d > 4$, elles ne se croisent qu'avec une probabilité strictement positive (qui tend vers 0 lorsque les deux points de départ sont pris éloignés l'un de l'autre) ; si elles se croisent, elles n'ont qu'un nombre fini de points d'intersection. En dimension $d = 4$, la probabilité que deux marches aléatoires qui démarrent à une distance d'ordre M l'une de l'autre se croisent décroît comme $1/\log \mathrm{M}$, mais l'*espérance* du nombre de fois où elles se croisent reste d'ordre 1 lorsque $\mathrm{M} \to \infty$. Cela montre que si elles se croisent, le nombre de points d'intersection est généralement assez grand, de l'ordre de $\log \mathrm{M}$.

L'essentiel du travail effectué dans [3] consiste à montrer que les chemins aléatoires issus de la représentation en amas aléatoires du

modèle d'Ising au point critique présentent un comportement similaire, mais avec $\log M$ remplacé par une quantité de taille au moins égale à $(\log M)^c$ pour un certain $c > 0$. L'argumentation est un chef-d'œuvre qui combine une analyse multi-échelle délicate, des arguments topologiques et un raisonnement probabiliste. L'un des principaux problèmes que les auteurs ont dû surmonter est le fait que ces chemins aléatoires sont très loin d'être de simples marches aléatoires et ne satisfont qu'une version spatiale de la propriété de Markov.

4 Invariance par rotation pour les modèles FK critiques

Comme on l'a déjà mentionné à plusieurs reprises, une caractéristique cruciale de la physique statistique à l'équilibre en dimension 2 est le fait que la plupart des modèles sont censés obéir à une forme d'invariance conforme (ou d'équivariance) lorsqu'on considère les observables à grande échelle à la température critique. Cette attente et le lien qui en résulte avec le monde bien étudié des théories conformes des champs en dimension 2 permettent de formuler une multitude de conjectures sur le comportement à grande échelle de ces modèles, mais ces conjectures sont souvent extrêmement difficiles à démontrer. Considérons par exemple la marche aléatoire auto-évitante à N pas en dimension 2 qui est simplement la mesure uniforme sur toutes les fonctions $h\colon \{0,\dots,N\} \to \mathbb{Z}^2$ telles que $h(0) = 0$ et telles que $|h(i+1)-h(i)| = 1$ pour tout $i < N$. En exploitant l'invariance conforme attendue de sa limite pour N grand convenablement normalisée, on s'attend à ce que la taille de $h(N)$ soit d'ordre $N^{3/4}$ et que sa mise à l'échelle en divisant par $N^{3/4}$ converge vers une courbe aléatoire continue particulière, à savoir $SLE_{8/3}$ [42]. D'un point de vue rigoureux, on ne sait presque rien de non trivial : bien que le diamètre de l'image de h doive trivialement être au moins $\sqrt{N/\pi}$, la meilleure minoration actuelle sur le point d'arrivée ne correspond même pas à cela ! Au lieu de cela, on ne connaît que l'inégalité $(\mathbb{E}|h(N)|^p)^{1/p} \geqslant \frac{1}{6}N^{p/(2p+2)}$ récemment obtenue par Madras [44]. De même, alors que l'inégalité $|h(N)| \leqslant N$ est triviale, la meilleure majoration non triviale est pratiquement la plus faible amélioration possible, à savoir que pour tout $p \geqslant 1$ on a $\lim_{N\to\infty} N^{-1}(\mathbb{E}|h(N)|^p)^{1/p} = 0$, obtenue à peu près au même moment par Duminil-Copin et Hammond [18]. L'un des principaux obstacles est qu'il n'existe actuellement aucune démonstration qui montre que la marche aléatoire auto-évitante présente une invariance conforme à grande échelle.

Bien que cela illustre l'importance de montrer que les modèles

statistiques présentent une invariance conforme (ou au moins une invariance par rotation, première étape cruciale) au point critique, la stratégie de démonstration de ces affirmations s'est jusqu'à présent principalement appuyée sur la recherche d'un ensemble suffisamment important d'observables qui vérifient un analogue discret de l'invariance conforme, généralement en résolvant un analogue discret des équations de Cauchy-Riemann. Voir par exemple la démonstration par Chelkak et Smirnov de l'invariance conforme pour le modèle d'Ising sur les graphes isoradiaux [15] et la démonstration par Smirnov de l'invariance conforme pour la percolation critique [56]. Le modèle FK en dimension 2 avec $q \leqslant 4$ déjà mentionné dans la section 2 est l'un des modèles les plus simples où l'invariance conforme au point critique est attendue, mais où l'on ne sait pas comment l'obtenir à partir d'une invariance conforme discrète convenable. Dans un travail récent [19], Duminil-Copin et ses collaborateurs ont montré que le comportement à grande échelle de ces modèles est invariant par rotation.

Pour définir la notion de « comportement à grande échelle », rappelons que l'espace des configurations du modèle FK est le même que celui de la percolation régulière (voir figure 1). Une telle configuration peut également être décrite comme un ensemble de boucles sans auto-intersection qui séparent les amas de percolation des amas de la configuration duale[3]. Étant donné deux ensembles $\mathcal{F}$ et $\bar{\mathcal{F}}$ de boucles sans auto-intersection dans le plan, on définit alors une distance entre elles de la manière suivante. Étant donné $\eta > 0$ (petit), on note $\mathcal{B}_\eta \subset \mathbb{R}^2$ un grand morceau d'un réseau fin dans $\mathbb{R}^2$, par exemple $\mathcal{B}_\eta = \eta\mathbb{Z}^2 \cap [-\eta^{-1}, \eta^{-1}]^2$. Étant donné une boucle γ et en supposant que son image ne coupe pas l'ensemble $\mathcal{B}_\eta$, on désigne alors par $[\eta]_\gamma$ sa classe d'homotopie dans $\mathbb{R}^2 \setminus \mathcal{B}_\eta$. On postule alors que $d_{\mathrm{H}}(\mathcal{F}, \bar{\mathcal{F}}) \leqslant \eta$ si et seulement si, pour tout $\gamma \in \mathcal{F}$ qui contient au moins deux éléments de $\mathcal{B}_\eta$ mais pas tous, il existe $\bar{\gamma} \in \bar{\mathcal{F}}$ tel que $[\gamma]_\eta = [\bar{\gamma}]_\eta$ et *vice versa*. Le H signifie ici « homotopie ».

Étant donné un espace métrique (M, d), la distance d se relève naturellement en une distance sur l'espace des mesures de probabilité sur M qui respecte la topologie de la convergence faible (au moins quand M est « gentil », par exemple polonais). Cela se fait en considérant la distance de Wasserstein (dite aussi de Kantorovitch-Rubinstein ou

3. En fait, elle produit naturellement *deux* ensembles de boucles, selon que la boucle entoure un amas de percolation de la configuration primaire ou de la configuration duale, mais nous ne tiendrons pas compte de ce détail dans le cadre de notre exposé.

de Monge-Kantorovitch)

$$d(\mu,\nu) = \inf_{\mathbb{P}\in C(\mu,\nu)} \int d(x,y)\,\mathbb{P}(dx,dy)\ ,$$

où $C(\mu_1,\mu_2)$ désigne l'ensemble de tous les couplages entre μ_1 et μ_2, c'est-à-dire les mesures de probabilité sur M^2 dont la i-ième marginale est égale à μ_i. Notons qu'avec cette définition, l'application qui à x associe la mesure de probabilité δ_x concentrée en x est une isométrie.

Fixons maintenant une fois pour toutes $q \in [1,4]$ et considérons un domaine lisse, borné et simplement connexe $\Omega \subset \mathbb{R}^2$. Pour $\varepsilon > 0$, on note $\mathbb{P}_{\varepsilon,\Omega}$ la mesure FK critique (vue comme une mesure sur des ensembles de boucles) sur $\varepsilon\mathbb{Z}^2 \cap \Omega$ avec des conditions aux limites libres. Notons également $\mathbb{P}_\varepsilon$ la limite de $\mathbb{P}_{\varepsilon,\Omega}$ lorsque $\Omega \to \mathbb{R}^2$. Étant donné un angle $\theta \in \mathbb{R}$, notons également R_θ la rotation de θ, qui agit naturellement sur les boucles dans $\mathbb{R}^2$. L'invariance par rotation à grande échelle du modèle FK critique peut alors être formulée comme suit.

Théorème 5. *Pour tout domaine $\Omega \subset \mathbb{R}^2$ comme ci-dessus et tout angle θ, on a*

$$\lim_{\varepsilon\to 0} d_{\mathrm{H}}\Big(\mathrm{R}_\theta^*\mathbb{P}_{\varepsilon,\Omega}, \mathbb{P}_{\varepsilon,\mathrm{R}_\theta\Omega}\Big) = 0\ .$$

De plus, $\lim_{\varepsilon\to 0} d_{\mathrm{H}}(\mathrm{R}_\theta^*\mathbb{P}_\varepsilon, \mathbb{P}_\varepsilon) = 0$.

Nous nous concentrons uniquement sur le second énoncé, car il s'avère que le premier peut s'en déduire sans trop d'efforts. En fait, les auteurs de [19] montrent un type d'énoncé d'universalité pour le modèle FK sur les réseaux rectangulaires, mais sa formulation nécessite une certaine préparation. Nous commençons par définir une classe particulière de plongements isoradiaux du réseau carré bidimensionnel dans le plan. Rappelons qu'un graphe planaire plongé dans le plan est isoradial si, pour toute face f, il existe un cercle de rayon 1 qui contient tous les sommets de f. Par exemple, le plongement canonique du réseau carré est isoradial.

Étant donné une suite bi-infinie $\alpha\colon \mathbb{Z} \to \,]-\frac{\pi}{2},\frac{\pi}{2}[$, nous considérons l'application $\iota_\alpha\colon \mathbb{Z}^2 \to \mathbb{R}^2$ donnée par

$$\iota_\alpha\colon (x,y) \mapsto \Big(x + s_y, c_y\Big)\ ,$$

$$s_y = \sum_{k\in]0,y]} \sin(\alpha_k)\ , \quad c_y = \sum_{k\in]0,y]} \cos(\alpha_k)\ ,$$

avec la convention que pour $y < 0$, $\sum_{]0,y]} = -\sum_{]y,0]}$. Ceci définit un graphe isoradial $\mathrm{L}(\alpha)$ en considérant le plongement de $\{(x, y) : x + y \text{ pair}\}$ (joints par des arêtes diagonales) par ι_α (voir figure 3). Le graphe dual $\mathrm{L}^*(\alpha)$ de $\mathrm{L}(\alpha)$ est alors donné par le plongement de $\{(x, y) : x+y \text{ impair}\}$. Le « graphe en losanges » associé a pour sommets à la fois les sommets de $\mathrm{L}(\alpha)$ et les centres de ses faces, et ses arêtes sont données par toutes les paires (v, f) avec v un sommet et f une face telle que $v \in f$. Le graphe en losanges est simplement donné par le plongement du réseau habituel $\mathbb{Z}^2$ avec les arêtes les plus proches par ι_α.

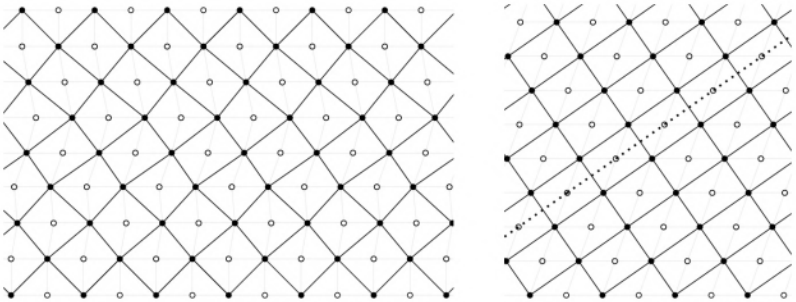


FIG. 3 – *Exemples de graphes* $\mathrm{L}(\alpha)$. *À gauche se trouve un* α *générique, tandis qu'à droite* α *est constant mais non nul. Le graphe lui-même est en noir, les sommets de son graphe dual sont en blanc, et le graphe en losange associé est en gris clair. En pointillé, on a tracé l'un des axes de symétrie du second graphe.*

Il est crucial à ce stade de noter que le modèle FK critique sur $\mathrm{L}(\alpha)$ n'est *pas* donné en considérant simplement l'image du modèle FK critique sur $\mathbb{Z}^2$ par l'application ι_α. Au lieu de cela, on repondère chaque arête du graphe d'une manière très particulière qui dépend de la longueur de l'arête. Plus précisément, si l'on considère une configuration du modèle FK comme un sous-ensemble $\omega \subset \mathrm{E}$ de l'ensemble des arêtes du graphe (fini) sur lequel le modèle est considéré, la probabilité de voir une configuration donnée ω est proportionnelle à

$$\left(\prod_{e\in\omega} p_e\right)\left(\prod_{e\in\mathrm{E}\setminus\omega}(1-p_e)\right)q^{k(\omega)}\,, \tag{12}$$

où $k(\omega)$ représente le nombre de composantes connexes du sous-

graphe ω. La formule pour p_e en fonction de q et de la longueur de l'arête e est explicite mais n'est pas pertinente dans le cadre de cette discussion.

L'étape la plus importante de la démonstration est de montrer que les propriétés de connectivité à grande échelle du modèle FK critique sur $\mathrm{L}(\alpha)$ sont très proches de celles du modèle sur $\mathrm{L}(\mathrm{T}_j\alpha)$, où T_j échange la j-ième et la $(j+1)$-ième composante :

$$(\mathrm{T}_j\alpha)_k = \begin{cases} \alpha_{j+1} & \text{si } k = j, \\ \alpha_j & \text{si } k = j+1, \\ \alpha_k & \text{sinon.} \end{cases}$$

En outre, il existe un couplage naturel entre les mesures FK sur les deux réseaux qui met en œuvre cette « fermeture ». Cette partie de la démonstration exploite le lien avec le modèle à six sommets et sa « résolubilité » à l'aide du formalisme des matrices de transfert. On en déduit alors que le modèle sur le réseau standard $\mathrm{L}(0)$ est très proche de celui sur un réseau rectangulaire tourné $\mathrm{L}(\alpha)$ avec $k \mapsto \alpha_k$ constant (voir la moitié droite de la figure 3). Cela fonctionne en fixant un grand $\mathrm{N} > 0$ (qui est ensuite envoyé à l'infini) et en partant de $\alpha_k^{(i)} = \alpha \mathbf{1}_{k \geqslant \mathrm{N}}$, puis en échangeant les composantes de manière à déplacer certaines des composantes non nulles vers le bas jusqu'à ce que l'on obtienne $\alpha_k^{(f)} = \alpha(\mathbf{1}_{|k| \leqslant \mathrm{N}} + \mathbf{1}_{k > 3\mathrm{N}})$. Comme on a $\mathrm{L}(0) \approx \mathrm{L}(\alpha^{(i)})$ et $\mathrm{L}(\alpha) \approx \mathrm{L}(\alpha^{(f)})$, l'énoncé souhaité s'ensuit si l'on peut contrôler l'erreur commise à chaque étape de l'algorithme. Cela s'avère extrêmement délicat et il faut exploiter de subtiles annulations stochastiques en cours de route. Une astuce consiste à permettre aux sommets de l'ensemble $\mathcal{B}_\eta$ autour duquel les classes d'homotopie sont calculées de se déplacer un peu à chaque application d'un opérateur de permutation T_j et de montrer que ce mouvement finit par être diffusif (et donc « lent ») plutôt que balistique.

Une fois que l'on sait que

$$\lim_{\varepsilon \to 0} d_{\mathrm{H}}(\mathbb{P}_{\varepsilon,\mathrm{L}(0)}, \mathbb{P}_{\varepsilon,\mathrm{L}(\alpha)}) = 0,$$

la seconde partie du théorème 5 s'ensuit immédiatement. L'idée est simplement de noter que $\mathrm{L}(\alpha)$ est invariant par réflexion le long d'une droite d'angle $\frac{\pi}{4} - \frac{\alpha}{2}$, mais que l'effet de cette réflexion sur $\mathrm{L}(0)$ est le même que celui d'une rotation d'angle α (puisqu'il est lui-même

invariant par réflexion le long d'une droite d'angle $\frac{\pi}{4}$), de sorte que

$$\begin{aligned} d_{\mathrm{H}}(\mathbb{P}_{\varepsilon}, \mathrm{R}_{\alpha}^{*}\mathbb{P}_{\varepsilon}) &\leqslant d_{\mathrm{H}}(\mathbb{P}_{\varepsilon,\mathrm{L}(0)}, \mathbb{P}_{\varepsilon,\mathrm{L}(\alpha)}) + d_{\mathrm{H}}(\mathbb{P}_{\varepsilon,\mathrm{L}(\alpha)}, \mathrm{R}_{\alpha}^{*}\mathbb{P}_{\varepsilon,\mathrm{L}(0)}) \\ &= 2d_{\mathrm{H}}(\mathbb{P}_{\varepsilon,\mathrm{L}(0)}, \mathbb{P}_{\varepsilon,\mathrm{L}(\alpha)}) \,. \end{aligned}$$

L'affirmation s'ensuit.

Financement. Ce travail a été partiellement soutenu par la Société royale de Londres grâce à une chaire de recherche.

Bibliographie

[1] *Phys. Rev. Lett.*, nº 47, 1981, p. 1-4.
[2] *Commun. Math. Phys.*, nº 86, 1982, p. 1-48.
[3] *Ann. Math.*, nº 194, 2021, p. 163-235
[4] *Commun. Math. Phys.*, nº 334, 2015, p. 719-742.
[5] *J. Stat. Phys.*, nº 44, 1986, p. 393-454.
[6] *J. Stat. Phys.*, nº 157, 2014, p. 692-742.
[7] *J. Stat. Phys.*, nº 159, 2015, p. 492-529.
[8] *Stud. Appl. Math.*, nº 50, 1971, p. 51-69.
[9] *J. Phys. C - Solid State*, nº 6, 1973, p. L445-L448.
[10] *J. Phys. A - Math. Gen.*, nº 9, 1976, p. 397-406.
[11] *Probab. Theory Rel. Fields*, nº 153, 2012, p. 511-542.
[12] *Math. Proc. Cambridge*, nº 53, 1957, p. 629–641.
[13] *Ann. Probab.*, nº 43, 2015, p. 528-571.
[14] *Ann. inst. H. Poincaré - Probab.*, nº 52, 2016, p. 146-161.
[15] *Invent. math.*, nº 189, 2012, p. 515-580.
[16] Duminil-Copin (Hugo), « 100 years of the (critical) Ising model on the hypercubic lattice », dans *Proceedings of the International Congress of Mathematicians*, Berlin, EMS Press, 2022, vol. I, p. 164-210.
[17] *Ann. sci. Éc. norm. supér.*, nº 54, 2021, p. 1363-1413.
[18] *Commun. Math. Phys.*, nº 324, 2013, p. 401-423.
[19] arXiv, 2012.11672.
[20] *Ann. Math.*, nº 189, 2019, p. 75-99.
[21] *Commun. Math. Phys.*, nº 349, 2017, p. 47-107.
[22] *Helv. Phys. Acta*, nº 44, 1971, p. 884-909.
[23] *Phys. Rev. D*, nº 86, 2012, article 025022.
[24] *J. Stat. Phys.*, nº 157, 2014, p. 869-914.
[25] *Commun. Math. Phys.*, nº 37, 1974, p. 93-120.
[26] *Commun. Math. Phys.*, nº 109, 1987, p. 437-480.

[27] *Ann. Phys.*, nº 97, 1976, p. 80-135.

[28] *Physica*, nº 57, 1972, p. 536-564.

[29] *Nuclear Phys. B*, nº 200, 1982, p. 281-296.

[30] *Commun. Math. Phys.*, nº 62, 1978, p. 1-34.

[31] *Commun. Math. Phys.*, nº 50, 1976, p. 79-95.

[32] *Phys. Rev. Lett.*, nº 54, 1985, p. 92-94.

[33] *Commun. Math. Phys.*, nº 10, 1968, p. 1-47.

[34] *Fortschr. Physik*, nº 21, 1973, p. 327-376.

[35] *J. Math. Phys.*, nº 11, 1970, p. 790-795.

[36] Grimmett (Geoffrey), *Percolation*, 2e éd., Springer, 1999.

[37] *Invent. math.*, nº 198, 2014, p. 269-504.

[38] *Ann. inst. H. Poincaré - Probab.*, nº 54, 2018, p. 1314-1340.

[39] *Probability and Phase Transition*, Dordrecht, Kluwer, 1994, p. 87-122.

[40] *J. Stat. Phys.*, nº 47, 1987, p. 99-121.

[41] *Z. Phys.*, nº 31, 1925, p. 253-258.

[42] *Fractal Geometry and Applications : A Jubilee of Benoît Mandelbrot, Part 2*, American Mathematical Society, 2004, p. 339-364.

[43] *Z. Phys.*, nº 21, 1920, p. 613-615.

[44] *Canad. Math. Bull.*, nº 57, 2014, p. 113-118.

[45] *Duke Math. J.*, nº 165, 2016, p. 3241-3378.

[46] *Commun. Pur. Appl. Math.*, nº 73, 2020, p. 2519-2555.

[47] *Mathematical Theory of Elementary Particles*, MIT Press, 1966, p. 69-73.

[48] *J. Funct. Anal.*, nº 12, 1973, p. 97-112.

[49] *46th Annual IEEE Symposium on Foundations of Computer Science*, 2005, p. 31-39.

[50] *Phys. Rev.*, nº 65, 1944, p. 117-149.

[51] *Commun. Math. Phys.*, nº 31, 1973, p. 83-112.

[52] *Commun. Math. Phys.*, nº 42, 1973, p. 281-305.

[53] *Proc. Cambridge Philos. Soc.*, nº 48, 1952, p. 106-109.

[54] *Commun. Math. Phys.*, nº 272, 2007, p. 283-344.

[55] *Israel J. Math.*, nº 118, 2000, p. 221-288.

[56] *Ann. Probab.*, nº 39, 2011, p. 1768-1814.

[57] Simon (Barry), *The* $P(\varphi)_2$ *Euclidean (quantum) field theory*. Princeton University Press, 1974.

[58] *Commun. Math. Phys.*, nº 33, 1973, p. 145-164.

[59] *Proc. Roy. Soc. London Ser. A*, nº 322, 1971, p. 251-280.

[60] *Phys. Rev.*, nº 85, 1952, p. 808-816.

Les travaux de June Huh (par Gil Kalai)

June Huh[1] *a trouvé des liens étonnants entre la géométrie algébrique et la combinatoire, résolu des problèmes centraux en combinatoire qui étaient restés ouverts pendant des décennies, et développé une théorie d'une grande importance pour les deux domaines. June Huh a reçu la médaille Fields 2022 « pour avoir apporté les idées de la théorie de Hodge à la combinatoire, pour la démonstration de la conjecture de Dowling-Wilson pour les treillis géométriques, pour la démonstration de la conjecture de Heron-Rota-Welsh pour les matroïdes, pour le développement de la théorie des polynômes lorentziens et pour la démonstration de la conjecture forte de Mason ». Dans cet article, je passerai en revue certaines des contributions de June Huh.*

June Huh a apporté des contributions fondamentales à la combinatoire et à la géométrie algébrique. Ses travaux ont permis d'établir des liens profonds entre ces deux domaines. Ce document décrit certaines des principales réalisations de Huh et donne quelques informations générales principalement sur les aspects combinatoires de son travail.

La conjecture d'unimodalité de Heron-Rota-Welsh [33,55,63] affirme que les coefficients du polynôme caractéristique d'un matroïde forment une suite log-concave. Cela implique que la suite des coefficients est unimodale. Un cas particulier de cette conjecture est une conjecture antérieure de Read, qui affirmait que les coefficients du polynôme chromatique d'un graphe sont unimodaux. En 2009, June Huh a utilisé la géométrie algébrique pour démontrer la conjecture d'unimodalité de Read [34] pour les graphes et la conjecture plus générale de Heron-Rota-Welsh pour les matroïdes représentés sur un corps de caractéristique nulle. Le cas des matroïdes représentables sur un corps de caractéristique non nulle et le cas des matroïdes généraux restaient ouverts. June Huh et Eric Katz [37] ont trouvé en 2010 une approche différente par la géométrie algébrique et ont résolu le cas des matroïdes représentables sur un corps de caractéristique quelconque. La conjecture de Heron-Rota-Welsh a été finalement démontrée en toute généralité en

Kalai (Gil), « The work of June Huh », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 50-65. DOI 10.4171/ICM2022/211

1. NDT. Avec le nom avant le prénom, on peut aussi écrire « Hŏ Jun-i » ou « Heo Jun-i », où le *u* se prononce *ou*.

2015 par Karim Adiprasito, June Huh et Eric Katz [2]. Pour ce faire, il était nécessaire d'étendre des théorèmes de géométrie algébrique (principalement les relations de Hodge-Riemann et le théorème de Lefschetz « difficile » [2]) à des cas qui dépassaient largement le cadre de la géométrie algébrique. Huh et ses coauteurs ont développé une théorie entièrement nouvelle d'un grand intérêt et d'une grande importance.

June Huh et Botong Wang [3] [39] ont utilisé des liens avec la géométrie algébrique pour démontrer la conjecture de Dowling-Wilson. Considérons une configuration P de n points qui engendrent un espace de dimension d. Soit w_i le nombre d'espaces vectoriels de dimension i engendrés par les points.

Motzkin a conjecturé dans sa thèse de doctorat de 1936 et démontré dans le cadre du corps des nombres réels en 1951 [49] que $w_1 \leqslant w_{d-1}$. Le cas $d = 3$ (dans une formulation de plan affine) a été démontré en 1948 par De Bruijn et Erdős. Leur démonstration combinatoire abstraite s'applique pour toute caractéristique.

La conjecture « *top heavy* » de Dowling-Wilson [22] affirme que

$$w_i \leqslant w_{d-i} \quad \text{si } i \leqslant [d/2].$$

Tom Braden, June Huh, Jacob Matherne, Nicholas Proudfoot et Botong Wang [12] ont démontré une généralisation de la conjecture de Dowling-Wilson pour des matroïdes arbitraires (de rang d).

La conjecture de Mason (sur les nombres d'indépendants) affirme [44] que la suite des nombres d'ensembles indépendants de taille k de matroïdes généraux est log-concave. Elle se décline en plusieurs niveaux. Suite au premier résultat de Huh, Mathias Lenz [42] a démontré la conjecture pour les matroïdes représentables sur les réels. Adiprasito [2] l'a démontrée pour les matroïdes généraux. June Huh, Benjamin Schröter et Botong Wang [38] ont démontré la conjecture de Mason forte pour les matroïdes arbitraires en s'appuyant sur [2].

Ces travaux ont conduit à d'autres avancées par plusieurs groupes de chercheurs. Je voudrais en particulier mentionner la solution par Anari, Oveis Gharan et Vinzant [4] de la conjecture de Mihail-Vazirani sur la constante d'expansion et le mélange rapide pour les marches aléatoires sur les matroïdes, ainsi que les travaux de Brändén et Huh [13] sur les inégalités de corrélation pour le modèle de Potts.

Nous discutons dans la section 1 des polynômes chromatiques et de la conjecture de Read, dans la section 2 des matroïdes et de la

2. NDT. Également appelé « théorème de Lefschetz vache ».
3. NDT. Le prénom est ici avant le nom, contrairement à la règle en chinois.

conjecture de Heron-Rota-Welsh, dans la section 3 de la conjecture de Dowling-Wilson. La section 4 est consacrée à la géométrie algébrique, à la théorie de Hodge et aux conjectures standard de Grothendieck. Dans la section 5, nous discutons des conjectures de Mason, de quelques applications et de liens récents. Andreï Okounkov [50] a écrit récemment un article de synthèse destiné au grand public sur les travaux de Huh et sur leur contexte mathématique.

1 Graphes, polynômes chromatiques et conjecture de Read

1.1 La conjecture des quatre couleurs et les polynômes chromatiques

Une coloration d'un graphe G est une coloration des sommets de G telle que deux sommets adjacents quelconques soient colorés avec des couleurs différentes. La coloration des graphes est d'une importance capitale dans la théorie des graphes et dans les algorithmes de graphes.

Théorème 1 (théorème des quatre couleurs, Appel et Haken, 1976)**.** *Tout graphe planaire peut être coloré avec quatre couleurs.*

La conjecture des quatre couleurs a été proposée (sous une forme duale pour les cartes planaires) par Francis Guthrie en 1852 et démontrée par Kenneth Appel et Wolfgang Haken en 1976.

Pour un graphe G, soit $\chi_G(k)$ le nombre de colorations de G avec k couleurs. On appelle $\chi_G(k)$ le polynôme chromatique du graphe G. Les polynômes chromatiques ont été introduits par George Birkhoff pour les cartes planaires comme outil possible pour l'étude de la conjecture des quatre couleurs. Hassler Whitney a étendu par la suite la définition aux graphes quelconques. William Tutte a trouvé une généralisation d'une grande portée, aujourd'hui appelée polynôme de Tutte. Il a également introduit les invariants de Tutte-Grothendieck pour les graphes, qui peuvent être considérés comme un pont précoce entre la théorie des graphes et la géométrie algébrique. Les opérations de suppression-contraction constituent l'un des points de départ des travaux de Tutte. Pour un graphe G et une arête e de G, désignons par $G\backslash e$ le graphe obtenu en supprimant l'arête e, et par G/e le graphe obtenu en contractant l'arête e, c'est-à-dire en fusionnant ses deux sommets en un seul sommet adjacent aux voisins des deux sommets. Il y a une relation fondamentale pour les polynômes chromatiques :

$$\chi_G(k) + \chi_{G/e}(k) = \chi_{G\backslash e}(k).$$

Cette relation conduit à une démonstration par récurrence facile du fait que le polynôme chromatique est bien un polynôme. Un graphe H est appelé un mineur d'un graphe G s'il peut être obtenu à partir de G par une suite de suppressions et de contractions. Richard Stanley a démontré [58] que $\chi_G(-1)$ est égal au nombre d'orientations acycliques de G.

1.2 La conjecture de Read

Ronald Read a proposé en 1968 la conjecture suivante. Si

$$\chi_G(x) = a_n x^n - a_{n-1}x^{n-1} + \cdots + (-1)^i a_{n-i}x^{n-i} + \cdots ,$$

alors la suite a_0, a_1, ..., a_n est unimodale.

Une conjecture beaucoup plus générale a été émise peu de temps après par Andrew Heron, Gian-Carlo Rota et Dominic Welsh. Ils ont également conjecturé une affirmation plus forte, à savoir que la suite des coefficients est en fait log-concave :

$$(a_k)^2 \geqslant a_{k-1}\, a_{k+1}, \quad k = 1, 2, \ldots, n-1.$$

Théorème 2 (June Huh [34])**.** *La suite des coefficients du polynôme chromatique $\chi_G(x)$ de tout graphe G est log-concave.*

De nombreux chercheurs ont étudié l'unimodalité et la log-concavité de suites issues de la combinatoire et de l'algèbre. Dans ce contexte, j'aimerais renvoyer le lecteur aux articles de synthèse [15, 16, 61]. Une propriété plus forte que la log-concavité des coefficients des polynômes réels est celle de n'avoir que des racines réelles. Ce n'est pas le cas des polynômes chromatiques des graphes en général (mais la localisation des racines reste un sujet fascinant). L'unimodalité des nombres d'éléments en fonction de leur hauteur dans les ensembles partiellement ordonnés gradués généraux est également liée à l'importante « propriété de Sperner » des ensembles partiellement ordonnés. Remarquons qu'il existe des cas où l'unimodalité attendue ne s'est pas vérifiée, par exemple l'unimodalité des nombres de faces des polytopes [11] et des treillis de Young [62].

J'ai entendu parler pour la première fois de la démonstration surprenante de Huh de la conjecture de Read dans un article de 2011 de Jiří Matoušek [45], qui considérait ce résultat parmi quelques autres comme le début d'une nouvelle ère en géométrie discrète et qui écrivait :

> « Pour moi, 2010 ressemble à une année miraculeuse dans plusieurs domaines parmi mes centres d'intérêt en mathématiques. J'énumère ci-dessous sept faits marquants et percées, principalement dans le domaine de la géométrie discrète, en espérant partager un peu de mon émerveillement et de mon plaisir avec les lecteurs. »

La démonstration de Huh s'appuie sur des liens entre le problème et les singularités des fonctions localement analytiques, et finalement les multiplicités mixtes de certains idéaux. Dans sa démonstration, Huh a relié les coefficients du polynôme chromatique aux nombres de Milnor d'un arrangement d'hyperplans complexes associé au graphe G. Comme nous le verrons dans la section suivante, sa démonstration se généralise à des arrangements d'hyperplans complexes arbitraires. Le lien établi par Huh entre les polynômes chromatiques des graphes et la géométrie algébrique a été d'une part une surprise totale, mais il était lié d'autre part à plusieurs développements autour de la combinatoire algébrique qui dataient du milieu des années soixante-dix. Les découvertes ultérieures de Huh, où il a appliqué la géométrie algébrique et en particulier la théorie de Hodge à la combinatoire, ont magnifiquement combiné des idées nouvelles et anciennes.

2 Les matroïdes et la conjecture de Heron-Rota-Welsh

2.1 Les matroïdes

Soit $X = \{x_1, x_2, \ldots, x_n\}$ un ensemble de points dans un espace vectoriel quelconque. On peut associer à X :

— l'ensemble des indépendants (c'est-à-dire des sous-ensembles linéairement indépendants) de X ;
— l'ensemble des bases de X (une base est un ensemble indépendant maximal) ;
— l'ensemble des circuits de X (un circuit est un ensemble dépendant minimal) ;
— l'ensemble des fermés [4] de X (un fermé est un sous-ensemble qui est stable par combinaison linéaire) ;

4. NDT. Voir : Gioan (Emeric) et Ramírez Alfonsín (Jorge), « Éléments de théorie des matroïdes et matroïdes orientés », dans *Informatique mathématique : une photographie en 2013*, Presses universitaires de Perpignan, 2013. On peut trouver également en français « l'ensemble des plats ».

— la fonction rang qui associe à un sous-ensemble Y de X la dimension de l'espace vectoriel engendré par Y.

Les matroïdes ont été introduits par Hassler Whitney [65] comme une généralisation des configurations de points dans les espaces vectoriels ou comme une abstraction de la notion de dépendance linéaire. La théorie des matroïdes est un exemple d'abstraction très réussie et une source d'exemples très utiles et explicites. La théorie des matroïdes a plusieurs liens avec la théorie des algorithmes, avec l'optimisation, ainsi qu'avec la logique mathématique.

Chacune des cinq notions que nous avons mentionnées plus haut (les indépendants, les bases, les circuits, les fermés et la fonction rang) donne lieu à une définition axiomatique des matroïdes. Toutes ces définitions axiomatiques sont équivalentes. La définition des matroïdes basée sur les indépendants est donnée par les propriétés suivantes :

1. Les sous-ensembles d'indépendants sont eux-mêmes indépendants.
2. Pour tout sous-ensemble Y de X, tous les indépendants maximaux de Y ont le même cardinal.

La première propriété signifie que l'ensemble des indépendants est un complexe simplicial abstrait, tandis que la seconde affirme que, pour tout sous-ensemble Y de l'ensemble X, le complexe induit sur Y est pur.

Pour un complexe simplicial abstrait K sur un ensemble X, nous pouvons définir son dual

$$K^* = \{S \subset X : X \backslash S \not\subset M\}.$$

Si M est un matroïde, nous pouvons définir son dual comme le matroïde dont le complexe d'indépendants est le dual du complexe d'indépendants de M.

2.2 Des graphes aux matroïdes

Soit G un graphe (connexe) à n sommets $\{v_1, v_2, \ldots, v_n\}$. Supposons que e_1, e_2, ..., e_n soit la base standard dans un espace vectoriel de dimension n sur un corps F. Nous associons à chaque arête $e = \{v_i, v_j\}$ avec $i < j$ le vecteur $e_i - e_j$. De manière remarquable, nous obtenons le même matroïde quel que soit le corps avec lequel nous commençons. Ce matroïde est appelé le matroïde graphique associé à G. Il est facile de voir dans ce cas que les bases correspondent à des arbres couvrants, que les circuits correspondent à des cycles élémentaires, que les indépendants

correspondent à des forêts couvrantes, et que la fonction rang pour le sous-graphe H qui correspond à un ensemble d'arêtes vaut n moins le nombre de composantes connexes de H.

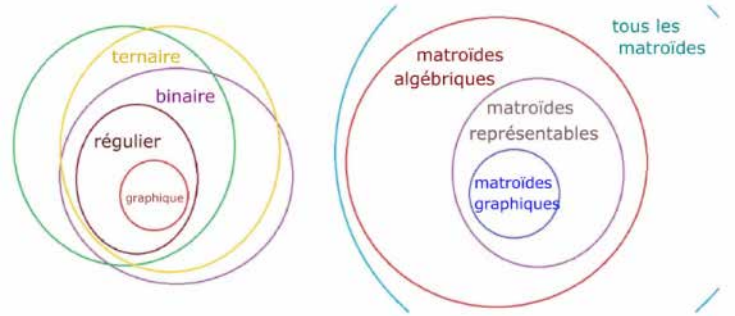


FIG. 1 – *Des classes importantes de matroïdes. À droite : Les matroïdes fournissent également une abstraction de la notion de dépendance algébrique. La grande et mystérieuse classe des matroïdes algébriques se compose de matroïdes qui peuvent être représentés par des relations de dépendance algébrique sur un certain corps. À gauche : Tutte a caractérisé les matroïdes graphiques en termes de mineurs interdits. Les matroïdes réguliers sont les matroïdes qui peuvent être représentés sur tous les corps ; Paul Seymour [57] a développé une théorie structurelle pour cette classe. Jim Geelen, Bert Gerards et Geoff Whittle (voir [28]) ont récemment démontré que, pour tout corps fini, les matroïdes représentés sur ce corps sont caractérisés par une liste finie de mineurs interdits.*

Si M est un matroïde graphique, le matroïde dual peut ne pas être graphique. Pour les graphes planaires cependant, le matroïde dual est le matroïde associé au graphe dual. Les notions de suppression et de contraction se généralisent de la théorie des graphes à la théorie des matroïdes. Ces deux opérations sont en effet duales dans le cadre de la dualité des matroïdes.

2.3 Fonction rang, polynômes caractéristiques et conjecture de Heron-Rota-Welsh

La fonction rang d'un matroïde associe un entier positif ou nul $r(Y)$ à chaque sous-ensemble $Y \subset X$, avec les propriétés suivantes :

(i) $r(\emptyset) = 0$,

(ii) $r(A \cup B) \leqslant r(A) + r(B) - r(A \cap B)$,

(iii) $r(A) \leqslant r(A \cup \{b\}) \leqslant r(A) + 1$.

Le polynôme caractéristique d'un matroïde M sur un ensemble X est défini par

$$\chi_M(\lambda) := \sum_{S \subseteq E} (-1)^{|S|} \lambda^{r(M)-r(S)}. \tag{1}$$

Si M est un matroïde graphique pour le graphe G, alors $\chi_M(\lambda)$ est le polynôme chromatique de G.

Théorème 3 (Adiprasito, Huh et Katz [2])**.** *Les coefficients du polynôme caractéristique d'un matroïde M sont log-concaves.*

June Huh [34] a démontré les résultats pour les matroïdes (considérés comme des arrangements d'hyperplans) représentables sur un corps de caractéristique nulle. Comme nous l'avons mentionné plus haut, la démonstration utilise les nombres de Milnor de l'arrangement. La démonstration de Huh et Katz [37] pour le cas d'une caractéristique quelconque repose sur la théorie de l'intersection de la « compactification magnifique » définie par Corrado De Concini et Claudio Procesi [21] pour les complémentaires d'arrangements d'hyperplans, combinée à une inégalité d'Askold Khovanskii et Bernard Teissier.

Adiprasito, Huh et Katz [2] ont démontré le résultat complet. Cela a nécessité une extension considérable des résultats de la géométrie algébrique aux anneaux de cohomologie de variétés algébriques qui n'existent pas. Voici la description de l'une des premières étapes de l'argumentation : la définition originale de De Concini et Procesi de la « compactification magnifique » s'appliquait aux matroïdes réalisables, mais Feichtner et Yuzvinsky ont défini en 2004 [25] un anneau commutatif associé à un matroïde arbitraire qui se réduit à l'anneau de cohomologie d'une compactification magnifique dans le cas réalisable.

Citons un extrait de [2] :

> « Après l'achèvement de [37], on s'est progressivement rendu compte que la validité des relations de Hodge-Riemann pour l'anneau de Chow de M était un ingrédient vital pour la démonstration des conjectures de log-concavité. Alors que l'anneau de Chow de M pouvait être défini pour un [matroïde] M arbitraire, la manière de formuler et de démontrer les relations de Hodge-Riemann n'était pas claire. Du point de vue de [25], l'anneau $A^*(M)_{\mathbb{R}}$ est l'anneau de Chow d'une variété torique lisse mais non compacte $X(\Sigma_M)$.

Il n'y a pas de moyen évident de se ramener au cas classique des variétés projectives. »

Nous discuterons de certains aspects liés à la géométrie algébrique dans la section 4. Remarquons que les résultats algébriques de [2] s'appliquent en fait à des objets géométriques plus généraux, bien au-delà des matroïdes.

3 La conjecture de Dowling-Wilson

3.1 Le contexte : les théorèmes de De Bruijn-Erdős, Motzkin, Greene et la démonstration par l'algèbre linéaire de Ryser

Théorème 4. *Un ensemble de n points du plan qui ne sont pas tous sur la même droite détermine au moins n droites.*

On dit ici qu'une configuration de points détermine une droite ℓ si la droite contient deux points (distincts) de la configuration.

Démonstration. D'après le théorème de Sylvester-Gallai, il existe une droite qui contient exactement deux points de la configuration. Le théorème en résulte par récurrence lorsque l'on supprime l'un de ces deux points de la configuration. □

Le théorème de Sylvester-Gallai ne s'applique pas en caractéristique deux, comme le montre le plan de Fano. Il ne s'applique pas non plus au plan complexe. En revanche, la démonstration de Nicolaas De Bruijn et Paul Erdős utilise un raisonnement combinatoire abstrait qui ne repose que sur le tout premier axiome d'Euclide : « par deux points distincts, il passe une droite et une seule. » Herbert Ryser [53] a donné une démonstration algébrique du théorème, que voici.

Démonstration. Considérons la matrice d'incidence (avec des 0 et des 1) dont les lignes correspondent aux points de la configuration et les colonnes aux droites déterminées par ces points. Notons $c_1, c_2, ..., c_m$ les colonnes de la matrice d'incidence. Remarquons que le produit scalaire de deux lignes distinctes est égal à 1. Notons $b_i = \langle c_i, c_i \rangle$ le nombre de points sur la i-ième ligne ($b_i > 1$). Supposons

$$\sum \alpha_i c_i = 0.$$

On écrit

$$0 = \langle \sum \alpha_i c_i, \sum \alpha_i c_i \rangle = \sum \alpha_i^2 (b_i - 1) + \Big(\sum \alpha_i \Big)^2 .$$

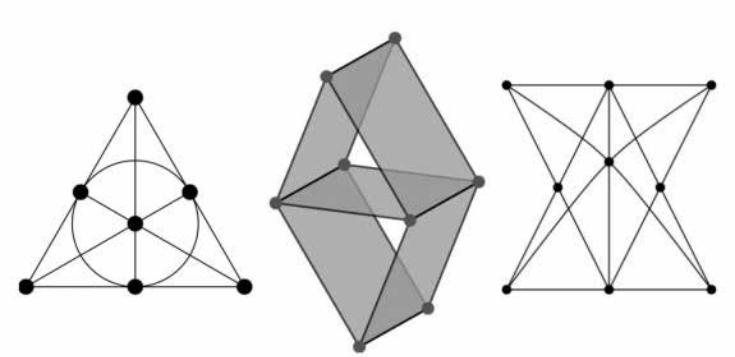


FIG. 2 – *Des exemples importants de matroïdes. De gauche à droite : le matroïde de Fano, le matroïde de Vámos et le matroïde non-Pappus. Les points du plan de Fano violent le théorème de Sylvester-Gallai et ne sont donc pas représentables sur les réels. En fait, le matroïde de Fano est représentable sur un corps F si et seulement si la caractéristique de F est 2. Le matroïde de Vámos n'est pas algébrique. L'antique théorème de Pappus implique que le matroïde non-Pappus n'est représentable sur aucun corps. Bernt Lindström a démontré qu'il est algébrique. Images de Wikipédia et du blogue* `matroidunion.org`.

On en déduit que les lignes sont linéairement indépendantes et donc que l'on doit avoir $m \leqslant n$. □

La démonstration de Ryser a été le point de départ de nombreuses démonstrations algébriques en combinatoire. Nous laissons comme exercice de montrer qu'elle implique qu'il existe une bijection $\psi(p)$ des points vers les droites telle que $p \in \psi(p)$.

Theodore Motzkin a étudié le théorème en dimensions supérieures. Il a conjecturé (déjà dans sa thèse de 1936) que n points dans un espace de dimension d qui engendrent de manière affine l'espace engendrent au moins n hyperplans. Motzkin lui-même a démontré le résultat ainsi qu'une généralisation du théorème de Sylvester-Gallai pour les configurations dans les espaces vectoriels réels de dimensions supérieures [49]. Curtis Greene [30] a démontré un théorème plus fort : il existe une bijection ψ de chaque point p vers un hyperplan qui contient p.

Passons maintenant aux matroïdes de rang d (notons que la dépendance affine des points dans un espace vectoriel de dimension d décrit un matroïde de rang $d+1$). En 1974, Thomas Dowling et Richard Wilson

ont conjecturé que

$$w_i \leqslant w_{d-i} \text{ si } i < d - i.$$

Cette conjecture est appelée « conjecture *top-heavy* ».

3.2 Démonstration de la conjecture de Dowling-Wilson

Théorème 5 (Braden, Huh, Matherne, Proudfoot et Wang, 2020 [12])**.** *Soit M un matroïde. Soit $\mathscr{L}^k(\mathrm{M})$ l'ensemble des fermés de rang k de M. Alors pour tout k et tout j tels que $k \leqslant j \leqslant \mathrm{rang}(\mathrm{M}) - k$,*

1. *Le cardinal de $\mathscr{L}^k(\mathrm{M})$ est au plus égal au cardinal de $\mathscr{L}^j(\mathrm{M})$.*
2. *Il existe une injection ψ de $\mathscr{L}^k(\mathrm{M})$ dans $\mathscr{L}^j(\mathrm{M})$ qui vérifie $\mathrm{F} \subset \psi(\mathrm{F})$.*

Un résultat supplémentaire du même article affirme que si Γ est un groupe quelconque agissant sur M, alors

3. *Il existe une injection ψ de $\mathbb{Q}\mathscr{L}^k(\mathrm{M})$ dans $\mathbb{Q}\mathscr{L}^j(\mathrm{M})$ de représentations de permutation de Γ.*

Le cas des matroïdes représentables a été démontré plus tôt par Huh et Wang en 2017 [39]. L'article [12] donne également des conséquences pour les polynômes de Kazhdan-Lusztig de matroïdes (introduits par Elias et Proudfoot).

Notons que la question de savoir si la suite $w_1, w_2, \ldots, w_n$ est log-concave reste ouverte, même pour les matroïdes représentables. On ne sait même pas pour les matroïdes de rang 3 si

$$w_2^2 \geqslant w_1 w_3.$$

C'est ce que l'on appelle la conjecture « points-droites-plans ». Une forme plus forte de cette conjecture (due à Mason) affirme que

$$w_2^2 \geqslant \frac{3}{2}\frac{w_1 - 1}{w_1 - 2} w_1 w_3.$$

En 1982, Paul Seymour [56] a démontré cette conjecture pour les matroïdes n'ayant pas cinq points sur une droite.

4 Le lien avec la théorie de Hodge et la géométrie algébrique

4.1 Trois idées fondamentales et autres ingrédients de la démonstration de la conjecture de Heron-Rota-Welsh

Lors d'une conférence à l'ICERM [5] en 2015, June Huh a déclaré :

5. NDT. « Institut de recherche numérique et expérimentale en mathématiques ».

« J'aime la solution encore plus que le problème. »

Dans cette conférence (voir aussi [36]), June Huh a expliqué trois idées fondamentales qui ont été utilisées dans la démonstration de la conjecture générale de Heron-Rota-Welsh :

1. L'idée de Bernd Sturmfels selon laquelle un matroïde peut être considéré comme un espace vectoriel tropical.

La géométrie tropicale a en effet fourni à la fois un cadre nécessaire et des indications sur la solution. En bref, les mathématiques tropicales remplacent l'addition traditionnelle par l'opération qui consiste à « prendre le minimum » et la multiplication par l'addition ordinaire. Cette idée est apparue dans plusieurs domaines des mathématiques et de la physique. Elle a joué un rôle important en géométrie énumérative (pour plus de détails, voir [36], la section 5.4 et l'appendice C de [50]).

2. L'idée de Richard Stanley selon laquelle une structure de Hodge polarisée sur la cohomologie des variétés toriques projectives conduit à d'importantes inégalités combinatoires.

Le principal exemple est le théorème *g* pour les polytopes convexes, pour lequel Stanley a utilisé le théorème de Lefschetz difficile pour l'anneau de cohomologie. Un autre exemple notable est la démonstration par Stanley de la conjecture d'Erdős-Moser.

3. L'idée de Peter McMullen selon laquelle la conjecture *g* peut être démontrée entièrement dans le cadre de la théorie des polytopes convexes en utilisant la « connexité par *flips* » des polytopes simpliciaux d'une dimension donnée.

Deux polytopes simpliciaux quelconques sont reliés par une suite de *flips* (également connus sous le nom de « mouvements de Pachner »). McMullen a démontré que la validité du théorème de Lefschetz difficile et des relations de Hodge-Riemann est préservée par les *flips*.

Dans la même conférence, June Huh a mentionné d'autres idées de personnes qui travaillent en combinatoire algébrique et en géométrie algébrique qui ont joué un rôle dans la démonstration. Nous avons déjà mentionné Tessier, Khovanskii, De Concini et Procesi, ainsi que Fleischer et Yuzvinsky. Huh a également mentionné Federico Ardila et Caroline Klivans [6], Angela Gibney et Diane Maclagan [29], Kalle Karu [40], et William Fulton et Robert MacPherson [26,27]. Bien entendu, la démonstration a impliqué un grand nombre d'idées originales supplémentaires (parfois folles) de la part d'Adiprasito, Huh et Katz eux-mêmes.

4.2 Dualité de Poincaré, théorème de Lefschetz difficile et relations de Hodge-Riemann

La théorie de Hodge donne lieu à trois conjectures, (DP), (LD) et (HR), appelées conjectures standard, pour certaines algèbres associées à des objets géométriques et combinatoires :

— (DP) signifie « dualité de Poincaré » et affirme que certains espaces vectoriels A_i et A_{d-i} sont duaux (et ont donc la même dimension) ;
— (LD) signifie « théorème de Lefschetz difficile » et affirme que certaines applications linéaires φ_k de A_k dans A_{k+1} ont la propriété que leur composition de A_i jusqu'à A_{d-i} est une injection ;
— (HR) signifie « relations de Hodge-Riemann ». (DP) et (LD) impliquent qu'une certaine forme bilinéaire est non dégénérée. (HR) est l'affirmation plus forte que cette forme est définie.

Dans le cas d'une variété algébrique projective lisse M, on peut considérer son anneau de cohomologie $A_i = H^{2i}(M)$. Pour le cas des variétés algébriques singulières, qui entrent en jeu dans les versions les plus fortes de la conjecture de Dowling-Wilson, il faut utiliser la cohomologie d'intersection.

June Huh a considéré dans [35] cinq exemples (nous sommes quelque peu imprécis ici) : la cohomologie d'une variété kählerienne compacte, l'anneau des cycles algébriques modulo l'équivalence homologique sur une variété projective lisse, l'algèbre de McMullen engendrée par les sommes de Minkowski d'un polytope convexe simple, la cohomologie d'intersection dans un cadre combinatoire d'un polytope convexe, le bimodule réduit de Soergel d'un élément d'un groupe de Coxeter, et l'anneau de Chow d'un matroïde. Le seul cas parmi ces exemples où les conjectures standard ne sont pas connues est leur apparition originale dans le travail de Grothendieck [31] sur les conjectures de Weil. L'exemple des bimodules de Soergel est lié à la célèbre solution en 2014 de la conjecture de Kazhdan-Lusztig pour les groupes de Coxeter généraux par Ben Elias et Geordie Williamson [23]. S'il est peut-être prématuré de l'attendre, il n'est pas prématuré d'espérer que des liens seront trouvés entre les apparitions combinatoires des conjectures standard et leurs apparitions en théorie des représentations et en théorie des nombres.

Remarques :

1. La démonstration de la conjecture de Heron-Rota-Welsh par June Huh et ses collaborateurs exploite largement la « positivité », à

savoir les relations de Hodge-Riemann. Pour un autre problème central de la combinatoire algébrique, la « conjecture g pour les sphères », la positivité n'est plus disponible. Des techniques remarquables pour la remplacer et ainsi démontrer la conjecture ont été récemment développées d'abord par Adiprasito [1] (la « propriété de Hall-Laman »), puis par Stavros Argyrios Papadakis et Vasiliki Petrotou [52] (la « propriété d'anisotropie ») et finalement par Adiprasito, Papadakis et Petrotou [3] (voir également Kalle Karu et Elizabeth Xiao [41] pour une démonstration simplifiée).

2. Les travaux de Karu [40] sur un théorème de Lefschetz difficile pour les polytopes généraux, ceux d'Elias et Williamson [23] sur la conjecture de Kazhdan-Lusztig et ceux de Braden, Huh, Matherne, Proudfoot et Wang [12] sur la conjecture de Dowling-Wilson s'appuient sur (LD) et (HR), non pas pour les extensions combinatoires de l'homologie ordinaire mais pour les extensions combinatoires de l'homologie d'intersection de Goresky et MacPherson.

5 Conjecture forte de Mason (sur les nombres d'indépendants), développements associés et applications

5.1 La conjecture de Mason et ses versions forte et ultra-forte

Soit M un matroïde à n éléments et soit $i_k(\mathrm{M})$ le nombre d'indépendants de M de taille k. La conjecture de Mason [44] se présente sous plusieurs formes :

— la conjecture de Mason

$$i_k^2(\mathrm{M}) \geqslant i_{k-1}(\mathrm{M})\, i_{k+1}(\mathrm{M})\,;$$

— la conjecture forte de Mason

$$i_k^2(\mathrm{M}) \geqslant \left(1+\frac{1}{k}\right) i_{k-1}(\mathrm{M})\, i_{k+1}(\mathrm{M})\,;$$

— la conjecture ultra-forte de Mason

$$i_k^2(\mathrm{M}) \geqslant \left(1+\frac{1}{k}\right)\left(1+\frac{1}{n-k}\right) i_{k-1}(\mathrm{M})\, i_{k+1}(\mathrm{M}).$$

Mathias Lenz a montré [42] comment obtenir la conjecture de Mason pour les matroïdes représentables en se basant sur les travaux de Huh et Katz. Adiprasito, Huh et Katz ont montré comment obtenir

la conjecture de Mason à partir de leurs techniques de théorie de Hodge. Huh, Schröter et Wang ont étendu ces techniques pour démontrer la conjecture de Mason forte. La conjecture ultra-forte a été démontrée en parallèle par Nima Anari, Kuikui Liu, Shayan Oveis Gharan et Cynthia Vinzant [5] avec un raisonnement combinatoire direct et par Brändén et Huh [13, 14] en s'appuyant sur la théorie de Hodge.

Les résultats obtenus par June Huh au cours de la dernière décennie ont donné lieu à de nombreuses recherches sur l'unimodalité et la log-concavité de diverses suites issues de la combinatoire. Dans certains cas, on a trouvé de nouvelles démonstrations combinatoires. On renvoie le lecteur aux articles récents de Swee Hong Chan et Igor Pak [19, 20].

5.2 La conjecture de Mihail-Vazirani

Pour un matroïde M sur un ensemble X, considérons un graphe dont les sommets sont toutes les bases de ce matroïde et tel que deux bases soient adjacentes si leur différence symétrique a deux éléments. Milena Mihail et Umesh Vazirani ont conjecturé que pour tout ensemble Y de sommets dans ce graphe, le nombre d'arêtes entre Y et son complémentaire $\bar{Y}$ est au moins $\min(|Y|, |\bar{Y}|)$.

Si M est constitué des éléments de la base standard dans $\mathbb{R}^d$ et de leurs opposés, alors le graphe que nous obtenons est le graphe du cube discret à n dimensions et l'assertion de la conjecture de Mihail-Vazirani est une inégalité isopérimétrique bien connue pour le cube discret.

Dans un article pionnier en 1992, Tomás Feder et Milena Mihail [24] ont démontré la conjecture pour les matroïdes équilibrés. Nima Anari, Shayan Oveis Gharan et Cynthia Vinzant [4] ont démontré en 2018 la conjecture de Mihail-Vazirani. Leur démonstration s'appuie sur l'article d'Adiprasito, Huh et Katz mais ils ont pu trouver progressivement des démonstrations élémentaires qui ne dépendent pas de la théorie de Hodge pour les inégalités cruciales dont ils avaient besoin. Leur résultat conduit à un algorithme en temps polynomial pour approcher le nombre de bases dans un matroïde.

Conclusion. Dans mon compte rendu, je me suis naturellement concentré sur l'aspect combinatoire de l'histoire. Je n'ai pas décrit le lien avec la géométrie tropicale, un domaine majeur à la fois en combinatoire algébrique et en géométrie algébrique. Le lecteur est également invité à consulter les articles de Huh pour en savoir plus sur la théorie des « polynômes lorentziens » développée par June Huh et

ses coauteurs.

C'est un grand plaisir de féliciter June Huh pour ses travaux spectaculaires.

Financement. Soutenu par la subvention 834735 du Conseil européen de la recherche et par la subvention ISF 2669/21.

Bibliographie

[1] arXiv, 1812.10454.

[2] *Ann. Math.*, nº 188, 2018, p. 381-452.

[3] arXiv, 2101.07245.

[4] *Duke Math. J.*, nº 170, 2021, p. 3459-3504.

[5] arXiv, 1811.01600.

[6] *J. Comb. Theory B*, nº 96, 2006, p. 38-49.

[7] *J. Am. Math. Soc.*, nº 36, 2023, p. 727-794.

[8] Appel (Kenneth) et Haken (Wolfgang), *Every Planar Map is Four Colorable*, American Mathematical Society, 1985.

[9] *Tohoku Math. J.*, nº 57, 2005, p. 273-292.

[10] *J. Comb. Theory A*, nº 31, 1981, p. 237-255.

[11] *Bull. Am. Math. Soc.*, nº 4, 1981, p. 187-188.

[12] arXiv, 2010.06088.

[13] arXiv, 1811.01696.

[14] arXiv, 1902.03719.

[15] Brenti (Francesco), *Unimodal, Log-concave and Pólya Frequency Sequences in Combinatorics*, American Mathematical Society, 1989.

[16] *Jerusalem Combinatorics '93*, American Mathematical Society, 1994, p. 71-89.

[17] *Indiana U. Math. J.*, nº 54, 2005, p. 263-307.

[18] *Ann. Math.*, nº 14, 1912, p. 42-46.

[19] arXiv, 2110.10740.

[20] arXiv, 2203.01533.

[21] *Sel. Math.*, nº 12, 1995, 459–494.

[22] *Proc. Am. Math. Soc.*, nº 47, 1975, p. 504-512.

[23] *Ann. Math.*, nº 180, 2014, p. 1089-1136.

[24] *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, ACM Press, 1992, p. 26-38.

[25] *Invent. math.*, nº 155, 2004, p. 515-536.

[26] *J. Algebraic Geom.*, nº 4, 1995, p. 181-193.

[27] *Topology*, nº 36, 1997, p. 335-353.

[28] *Not. Am. Math. Soc.*, nº 61, 2014, p. 736-743.

[29] *Int. Math. Res. Notices*, nº 14, 2012, p. 3224-3255.

[30] *J. Comb. Theory*, nº 9, 1970, p. 357-364.

[31] *Algebraic Geometry*, Oxford University Press, 1969, p. 193-199.

[32] *J. Comb. Theory B*, nº 47, 1989, p. 146-152.

[33] *Combinatorics*, Institute of Mathematics and Its Applications, 1972, p. 164-202.

[34] *J. Am. Math. Soc.*, nº 25, 2012, p. 907-927.

[35] *Proceedings of the International Congress of Mathematicians*, Singapour, World Scientific, 2018, vol. IV, p. 3093-3111.

[36] *Current Developments in Mathematics 2016*, Somerville, International Press, 2018, p. 1-46.

[37] *Math. Ann.*, nº 354, 2012, p. 1103-1116.

[38] *J. Eur. Math. Soc.*, nº 24, 2022, p. 1335-1351.

[39] *Acta Math.*, nº 218, 2017, p. 297-317.

[40] *Invent. math.*, nº 157, 2004, p. 419-447.

[41] arXiv, 2204.07758.

[42] *Adv. Appl. Math.*, nº 51, 2013, p. 543-545.

[43] *J. Comb. Theory B*, nº 28, 1980, p. 208-236.

[44] *Combinatorics*, Institute of Mathematics and its Applications, 1972, p. 207-220.

[45] Matoušek (Jiří), « The dawn of an algebraic era in discrete geometry ? », dans *Proceedings of the 27th European Workshop on Computational Geometry (EuroCG 2011)*.

[46] *Israel J. Math.*, nº 9, 1971, p. 559-570.

[47] *Invent. math.*, nº 113, 1993, p. 419-444.

[48] *Discrete Comput. Geom.*, nº 15, 1996, p. 363-388.

[49] *Trans. Am. Math. Soc.*, nº 70, 1951, p. 451-464.

[50] Okounkov (Andrei), « Combinatorial geometry takes the lead », dans *Proceedings of the International Congress of Mathematicians*, Berlin, EMS Press, 2022, vol. I, p. 414-458.

[51] Oxley (James), *Matroid Theory*, Oxford University Press, 2011.

[52] arXiv, 2012.09815.

[53] *J. Algebra*, nº 10, 1968, p. 246-261.

[54] *J. Combin. Theory*, nº 4, 1968, p. 52-71.

[55] *Actes du congrès international des mathématiciens*, Paris, Gauthier-Villars, 1971, tome III, p. 229-233.

[56] *J. Combin. Theory B*, nº 33, 1982, p. 17-26.

[57] *J. Combin. Theory B*, nº 28, 1980, p. 305-359.

[58] *Discrete Math.*, nº 5, 1973, p. 171-178.

[59] *Adv. Math.*, nº 35, 1980, p. 236-238.

[60] *Proceedings of the International Congress of Mathematicians*, Varsovie, PWN, 1984, vol. I-II, p. 447-453.

[61] *Graph Theory and its Applications : East and West*, New York Academy of sciences, 1989, p. 500-535.

[62] *J. Combin. Theory A*, nº 54, 1990, p. 41-53.

[63] *Combinatorial Mathematics and its Applications*, Londres, Academic Press, 1971, p. 291-306.

[64] Welsh (Dominic), *Matroid Theory*, Londres, Academic Press, 1976.

[65] *Am. J. Math.*, nº 57, 1935, p. 509-533.

Les travaux de James Maynard (par Kannan Soundararajan)

Nous présentons brièvement quelques-uns des résultats les plus spectaculaires obtenus par James Maynard, qui lui ont valu la médaille Fields.

James Maynard a obtenu plusieurs résultats spectaculaires en théorie analytique des nombres. Bien que les démonstrations de ces résultats fassent appel à de nombreuses idées profondes, leurs énoncés sont remarquables par leur simplicité et leur élégance. Pour illustrer notre propos, nous énonçons deux de ces résultats frappants de Maynard sur les nombres premiers, avant de les replacer dans leur contexte.

Théorème 1 (Maynard [32])**.** *Pour tout entier naturel $m \geqslant 2$, il existe un entier strictement positif $C(m)$ avec la propriété suivante : il existe une infinité d'entiers naturels n tels que l'intervalle $[n, n + C(m)]$ contienne au moins m nombres premiers.*

Théorème 2 (Maynard [36])**.** *Il existe une infinité de nombres premiers p dont l'écriture décimale ne contient pas le chiffre 7.*

1 Le contexte

Pour replacer ces résultats dans leur contexte, rappelons que le théorème des nombres premiers donne le comportement asymptotique du nombre $\pi(x)$ de nombres premiers inférieurs ou égaux à x, à savoir

$$\pi(x) \sim \mathrm{li}(x) = \int_0^x \frac{dt}{\log t}\,.$$

Nous pouvons considérer que ce résultat asymptotique revient à dire que la « probabilité » qu'un nombre n soit premier est d'environ $1/\log n$. L'un des thèmes principaux de la théorie analytique des nombres peut être formulé comme ceci : en quoi la suite des nombres premiers ressemble-t-elle ou diffère-t-elle d'une suite aléatoire d'entiers où chaque

Soundararajan (Kannan), « The work of James Maynard », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 66-80. DOI 10.4171/ICM2022/212

entier $n \geqslant 3$ serait choisi indépendamment pour faire partie de la suite aléatoire avec une probabilité $1/\log n$. Ceci est également connu sous le nom de « modèle de Cramér ». Une différence évidente est que tous les nombres premiers strictement supérieurs à 2 doivent être impairs, alors qu'une suite aléatoire contiendrait certainement de nombreux nombres pairs. Mais si nous pouvions tenir compte de la divisibilité par de petits nombres premiers (tels que 2 dans notre exemple), un modèle aléatoire modifié décrirait-il avec précision le comportement des nombres premiers ?

Il existe de nombreuses façons d'essayer de préciser ce thème. Par exemple, l'hypothèse de Riemann prédit que $|\pi(x) - \mathrm{li}(x)|$ est borné par $\mathrm{C}(\varepsilon)x^{\frac{1}{2}+\varepsilon}$ pour tout $\varepsilon > 0$ et pour une certaine constante $\mathrm{C}(\varepsilon)$. Des fluctuations dont la taille est de l'ordre de $\sqrt{x}$ sont en effet ce à quoi on peut s'attendre si l'on choisit des ensembles aléatoires d'entiers avec $n \geqslant 3$, inclus dans l'ensemble avec une probabilité $1/\log n$. L'hypothèse de Riemann est ainsi compatible à un niveau rudimentaire avec un modèle aléatoire des nombres premiers. Si nous examinions le terme d'erreur $\pi(x) - \mathrm{li}(x)$ plus en détail, l'influence des zéros de la fonction $\zeta(s)$ serait alors visible et de telles caractéristiques s'écarteraient (de manière faible mais significative) du modèle aléatoire.

Lors du congrès international des mathématiciens de 1912, Landau a mentionné quatre problèmes « inattaquables » sur les nombres premiers :

1. La conjecture de Goldbach selon laquelle tout nombre entier pair strictement supérieur à 2 est la somme de deux nombres premiers.
2. Le problème des nombres premiers jumeaux selon lequel il existe une infinité de paires de nombres premiers $(n, n+2)$.
3. Il existe toujours un nombre premier entre deux carrés consécutifs.
4. Il existe une infinité de nombres premiers de la forme $n^2 + 1$.

Ces quatre problèmes restent ouverts aujourd'hui. Tous les énoncés correspondent exactement à ce que l'on attendrait de suites aléatoires. Par exemple, le modèle de Cramér suggère que la probabilité que n et $n+2$ soient tous deux premiers est d'environ $[1/\log n] \times [1/\log(n+2)]$, ce qui permettrait de prédire environ $x/(\log x)^2$ nombres premiers jumeaux inférieurs à x. Il faut bien sûr faire attention, car on pourrait faire la même prédiction pour n et $n+1$ premiers. Nous y reviendrons. On peut s'attendre de même à ce qu'un nombre pair N ait environ $\mathrm{N}/(\log \mathrm{N})^2$ représentations en tant que somme de deux nombres premiers, ce qui rend la conjecture de Goldbach très plausible. Des arguments similaires suggèrent également les deux derniers problèmes de Landau.

Pour le troisième problème de Landau sur le nombre de nombres premiers entre n^2 et $(n+1)^2$, le modèle aléatoire prédit déjà ce que nous croyons être la bonne réponse, à savoir qu'il devrait y avoir environ $(2n+1)/\log(n^2) \approx n/\log n$ nombres premiers dans cet intervalle. Pour les trois autres problèmes, des modifications doivent être apportées au modèle de Cramér afin de prendre en compte les caractéristiques déterministes de ces problèmes en ce qui concerne la divisibilité par de petits nombres premiers. Des conjectures précises pour ces problèmes ont été formulées pour la première fois par Hardy et Littlewood, motivés par leurs travaux sur la méthode du cercle. Ces conjectures sont généralement considérées comme plausibles et sont étayées par de nombreuses observations heuristiques et numériques. Hardy et Littlewood ont par exemple formulé la conjecture suivante pour le nombre de nombres premiers jumeaux inférieurs à x :

$$\#\Big\{n \leqslant x : \quad n, n+2 \text{ premiers} \Big\} \sim \mathfrak{S}(\{0,2\}) \int_2^x \frac{dt}{(\log t)^2}.$$

Ici, $\int_2^x dt/(\log t)^2$ vaut asymptotiquement $x/(\log x)^2$ et correspond à la prédiction du modèle de Cramér, tandis que $\mathfrak{S}(\{0,2\})$ est un facteur de correction appelé « série singulière » :

$$\mathfrak{S}(\{0,2\}) = 2 \prod_{p \geqslant 3} \left(1 - \frac{2}{p}\right)\left(1 - \frac{1}{p}\right)^{-2} \approx 1{,}32\ldots$$

La constante $\mathfrak{S}(\{0,2\})$ a une interprétation probabiliste convaincante : c'est un produit sur tous les nombres premiers p (le premier facteur 2 correspond au nombre premier $p = 2$), avec le facteur correspondant à p qui suit le rapport entre la probabilité que n et $n+2$ ne soient pas divisibles par p et la probabilité que deux nombres aléatoires ne soient pas divisibles par p. Ainsi, pour $p = 2$, la probabilité que n et $n+2$ ne soient pas divisibles par 2 est $(1 - 1/2)$ (n doit être impair), tandis que la probabilité que deux nombres aléatoires ne soient pas divisibles par 2 est $(1 - 1/2)^2 = 1/4$; le rapport de ces probabilités donne le facteur de correction 2. Pour les nombres premiers $p \geqslant 3$, la probabilité que n et $n+2$ ne soient pas divisibles par p est $(1 - 2/p)$ alors que la probabilité que deux nombres aléatoires ne soient pas divisibles par p est $(1 - 1/p)^2$; nous voyons le facteur de correction correspondant dans la définition de $\mathfrak{S}(\{0,2\})$.

On peut faire des conjectures similaires pour le problème de Goldbach ou pour le nombre de nombres premiers de la forme $n^2 + 1$ en

modifiant et en corrigeant les prédictions naïves du modèle de Cramér. Pour illustrer notre propos, donnons une généralisation de la conjecture des nombres premiers jumeaux pour le comptage de k-uplets premiers : étant donné des entiers distincts $h_1, h_2, \ldots, h_k$, combien y a-t-il (pour x grand) d'entiers $n \leqslant x$ avec $n + h_1, \ldots, n + h_k$ qui sont tous premiers. La conjecture de Hardy-Littlewood prédit ici que

$$\#\Big\{n \leqslant x : \ \ n + h_1, \ldots, n + h_k \text{ tous premiers } \Big\} \sim \mathfrak{S}(\{h_1, \ldots, h_k\}) \int_2^x \frac{dt}{(\log t)^k},$$

où, avec $\mathcal{H} = \{h_1, \ldots, h_k\}$,

$$\mathfrak{S}(\mathcal{H}) = \prod_p \left(1 - \frac{\nu(\mathcal{H}, p)}{p}\right)\left(1 - \frac{1}{p}\right)^{-k} \tag{1}$$

et $\nu(\mathcal{H}, p)$ désigne le nombre de classes de résidus distinctes occupées par l'ensemble $\mathcal{H}$ vu modulo p. Puisque $\nu(\mathcal{H}, p) = k$ si p est plus grand que $\max |h_i - h_j|$, le produit qui définit $\mathfrak{S}(\mathcal{H})$ converge absolument vers un nombre réel positif ou nul, qui n'est égal à zéro que si $\nu(\mathcal{H}, p) = p$ pour un certain nombre premier p. Si $\nu(\mathcal{H}, p) = p$, alors pour tout entier n, au moins un des nombres $n + h_1, \ldots, n + h_k$ est un multiple de p, donc il ne peut y avoir qu'un nombre fini d'entiers n avec $n+h_1, \ldots, n+h_k$ tous premiers. Par exemple, c'est ce qui se passe si nous demandons que n et $n + 1$ soient premiers, ou que $n, n + 2, n + 4$ soient tous premiers. Lorsqu'il n'y a pas d'obstacle de divisibilité à ce que $n + h_1, \ldots, n + h_k$ soient premiers, la conjecture de Hardy-Littlewood prédit un grand nombre de k-uplets premiers. C'est peut-être la question la plus centrale de la théorie des nombres premiers. Elle reste ouverte dans toutes les situations où $\mathfrak{S}(\mathcal{H})$ est non nul.

2 Théorie des cribles

Nous avons décrit rapidement certaines des principales questions qui motivent la théorie des nombres premiers. L'une des principales sources de progrès vers ces questions est la théorie des cribles. Une grande partie du travail de Maynard se situe essentiellement dans ce domaine. Un problème typique de la théorie des cribles est de majorer ou minorer la taille des ensembles d'entiers $\mathcal{A}$ dont les éléments sont contraints d'omettre $\nu(p)$ classes de résidus modulo p pour des nombres premiers p. Par exemple, le problème des nombres premiers jumeaux

est de cette forme puisque nous cherchons à trouver des entiers n qui ne sont congrus ni à 0 ni à -2 modulo p pour tous les nombres premiers $p \leqslant \sqrt{n+2}$ (de sorte que n et $n+2$ seraient tous les deux premiers). En général, les méthodes de crible peuvent produire des majorants de l'ordre de grandeur conjecturé. On peut montrer par exemple que le nombre de nombres premiers jumeaux inférieurs à x n'est pas plus de 4 fois l'asymptotique de Hardy-Littlewood conjecturée. L'obtention de minorants correspondants s'est avérée être un problème beaucoup plus difficile, mais les méthodes de crible ont conduit à des résultats partiels frappants tels que le théorème de Chen selon lequel il existe de nombreux nombres premiers p pour lesquels $p+2$ a au plus deux facteurs premiers, ou le théorème d'Iwaniec selon lequel il existe de nombreux nombres n pour lesquels n^2+1 a au plus deux facteurs premiers. Pour un traitement complet du sujet, voir [14].

Le théorème de Chen et le théorème d'Iwaniec mettent en évidence une limitation des méthodes traditionnelles de crible, connue sous le nom de *problème de parité*, qui nous empêche souvent de connaître la parité des éléments non criblés et donc d'obtenir des nombres premiers. Mais les méthodes de crible, en conjonction avec d'autres apports analytiques, ont permis d'obtenir des nombres premiers dans certains cas particuliers. Par exemple pour x grand, Baker, Harman et Pintz [2] ont montré que l'intervalle $[x, x+x^\theta]$ contient au moins $cx^\theta/\log x$ nombres premiers, où $c>0$ est une constante et $\theta = 0{,}525$. Le problème de Landau pour trouver des nombres premiers entre des carrés consécutifs correspond à des intervalles avec $\theta = \frac{1}{2}$. Un autre exemple spectaculaire est dû à Friedlander et Iwaniec [13], qui ont établi une formule asymptotique pour le nombre de nombres premiers inférieurs à x qui peuvent être écrits sous la forme n^2+m^4, une approximation du problème de Landau relatif aux nombres premiers de la forme n^2+1. Un résultat très proche de Heath-Brown et Li [25] donne une formule asymptotique pour les nombres premiers de la forme n^2+p^4, où p est un nombre premier. Un autre beau résultat dû à Heath-Brown [24] établit une formule asymptotique pour le nombre de nombres premiers inférieurs à x de la forme n^3+2m^3 avec $m, n \in \mathbb{N}$. Le résultat de Heath-Brown peut être considéré comme une approximation du problème qui consiste à obtenir des nombres premiers de la forme n^3+2. Mais avant ses travaux, on ne savait même pas s'il existait un nombre infini de nombres premiers qui étaient la somme de trois cubes d'entiers naturels ! Une caractéristique cruciale de ces résultats est qu'ils traitent des nombres premiers représentés par des cas particuliers

de *normes*. Le résultat de Friedlander et Iwaniec concerne la norme $x^2 + y^2 = \mathrm{N}(x + iy)$ associée au corps $\mathbb{Q}(i)$ dans le cas particulier où y est un carré. Le résultat de Heath-Brown concerne la norme $\mathrm{N}(x + y\alpha + z\alpha^2)$, qui prend la norme sur le corps $\mathbb{Q}(\alpha)$ avec $\alpha = 2^{\frac{1}{3}}$, dans le cas particulier où z est égal à 0. Les résultats de Friedlander et Iwaniec et de Heath-Brown ont donné les premiers exemples de suites « fines » (au sens où le nombre d'entiers inférieurs à X dans la suite est $\leqslant \mathrm{X}^{1-\delta}$ pour un certain $\delta > 0$) de valeurs polynomiales en deux variables ou plus qui représentent une infinité de nombres premiers. On ne connaît aucun exemple de polynôme en une variable de degré supérieur à 1 qui représente une infinité de nombres premiers.

Le travail de Maynard [40] donne une généralisation substantielle de l'approche de Heath-Brown et produit de nombreux autres exemples de suites fines de valeurs polynomiales en plusieurs variables qui représentent des nombres premiers. Considérons un nombre algébrique $\omega \in \mathbb{C}$ de degré n et notons K le corps $\mathbb{Q}(\omega)$. On peut lui associer la norme $\mathrm{N}(\sum_{i=1}^{n} x_i \omega^{i-1})$, qui est un polynôme homogène de degré n en les variables $x_1, \ldots, x_n$. On obtiendrait un polynôme fin en plusieurs variables en spécialisant certaines des variables de cette norme pour qu'elles soient nulles. En fixant par exemple $x_{n-k+1}, \ldots, x_n = 0$, le nombre d'entiers inférieurs à x représentés par une telle norme incomplète serait d'environ $x^{1-k/n}$. Dans l'intervalle $n \geqslant 4k$, Maynard a établi une formule asymptotique pour le nombre de nombres premiers représentés par une telle norme incomplète lorsque les variables $x_1, \ldots, x_{n-k}$ prennent des valeurs entières dans l'intervalle $[1, \mathrm{X}]$.

3 La méthode du cercle

Outre la théorie des cribles, une autre source importante de progrès dans la résolution de problèmes sur les nombres premiers est la méthode du cercle, qui a été comme nous l'avons déjà mentionné la motivation initiale de Hardy et Littlewood dans la formulation de leurs conjectures. Pour illustrer cela, considérons le problème de Goldbach qui consiste à représenter un entier pair N comme une somme de deux nombres premiers. En utilisant l'analyse harmonique, le nombre de telles représentations de N peut être écrit sous la forme

$$r(\mathrm{N}) = \int_0^1 \mathrm{S}(\alpha)^2 \, e^{-2\pi i \mathrm{N}\alpha} d\alpha, \quad \text{où} \quad \mathrm{S}(\alpha) = \sum_{p \leqslant \mathrm{N}} e^{2\pi i p \alpha}. \tag{2}$$

L'idée de la méthode du cercle est que les fonctions génératrices telles que $S(\alpha)$ ont tendance à être grandes près des nombres rationnels à petit dénominateur (les *arcs majeurs*) et petites loin d'eux (les *arcs mineurs*).

Si la méthode du cercle n'a pas permis de résoudre le problème de Goldbach ou le problème des nombres premiers jumeaux, elle s'est avérée extrêmement efficace dans les problèmes où l'on dispose d'un peu plus de liberté. Par exemple, la conjecture faible de Goldbach demande de représenter les nombres impairs comme une somme de trois nombres premiers. Il y a ici une variable supplémentaire avec laquelle jouer. Vinogradov a utilisé la méthode du cercle pour montrer que tous les grands nombres impairs sont la somme de trois nombres premiers. Helfgott [26] a étendu cette méthode pour montrer que tous les nombres impairs plus grands que 5 peuvent être représentés de cette manière. Nous pouvons mentionner ici un résultat impressionnant de Matomäki, Maynard et Shao [30] qui montre que les grands nombres impairs n peuvent s'écrire sous la forme $p_1+p_2+p_3$, où les trois nombres premiers p_i se trouvent dans un court intervalle $[n/3 - n^\theta, n/3 + n^\theta]$ pour n'importe quel $\theta > 11/20$. Nous avons mentionné précédemment les travaux de Baker, Harman et Pintz [2] qui montrent l'existence de nombres premiers dans des intervalles courts $[x, x + x^{0,525}]$. Les résultats de [30] sont remarquables pour résoudre la conjecture faible de Goldbach en utilisant des nombres premiers dans des intervalles à peine plus longs.

Un deuxième exemple de ce que pourrait signifier un degré de liberté supplémentaire est le théorème de Green-Tao selon lequel l'ensemble des nombres premiers contient des progressions arithmétiques arbitrairement longues $n, n + d, \ldots, n + (k - 1)d$. La conjecture de Hardy-Littlewood prédit une version « unidimensionnelle » plus forte de ce résultat avec des choix particuliers pour la raison d. Par exemple, il devrait y avoir une infinité de k-uplets premiers de la forme $n, n + k!$, $n + 2 \cdot k!, \ldots, n + (k - 1) \cdot k!$. Les travaux de Green, Tao et Ziegler [19–21] peuvent être considérés comme une généralisation de grande portée de la méthode du cercle qui permet d'obtenir des formules asymptotiques pour le nombre de solutions en nombres premiers de systèmes linéaires avec « au moins deux degrés de liberté ».

Le magnifique résultat de Maynard sur les nombres premiers avec des chiffres manquants (théorème 2 ci-dessus) est un cas rare où la méthode du cercle peut être utilisée pour résoudre un problème binaire. Soit $\mathcal{M}$ l'ensemble des entiers naturels sans 7 dans leur écriture décimale (on pourrait naturellement omettre n'importe quel autre chiffre au lieu

de 7). Le nombre d'entiers jusqu'à N qui sont dans $\mathcal{M}$ est environ $N^{\log 9/\log 10} = N^{1-\delta}$ avec $\delta = 0{,}046\ldots$, de sorte que $\mathcal{M}$ est un ensemble fin, ce qui rend difficile le problème de trouver des nombres premiers dans cet ensemble. Avant les travaux de Maynard, Dartyge et Mauduit [7, 8] avaient utilisé la théorie des cribles pour montrer que $\mathcal{M}$ contient une infinité d'entiers avec au plus deux facteurs premiers. Pour compter le nombre de facteurs premiers dans $\mathcal{M}$ jusqu'à N, on utilise l'analyse harmonique pour écrire

$$\sum_{\substack{p\leqslant N\\ p\in\mathcal{M}}} 1 = \int_0^1 S(\alpha)\, M(-\alpha)\, d\alpha,$$

où $S(\alpha)$ est la somme exponentielle sur les nombres premiers définie en (2) et où

$$M(\alpha) = \sum_{m\leqslant N, m\in\mathcal{M}} e^{2\pi i\alpha}$$

est la somme exponentielle correspondante sur l'ensemble $\mathcal{M}$. Il est habituellement impossible de s'attaquer à un tel problème binaire par la méthode du cercle. Car même en étant le plus optimiste possible, nous ne pouvons espérer qu'une « compensation en racine carrée » dans les sommes exponentielles $S(\alpha)$ et $M(-\alpha)$ pour un α générique. Même cela produirait un intégrande de taille $N^{\frac{1}{2}} \times N^{\frac{1}{2}(1-\delta)}$, ce qui est plus grand que le terme principal attendu d'une taille d'environ $N^{1-\delta}/\log N$. Une caractéristique cruciale de ce problème est que l'ensemble $\mathcal{M}$ a une structure très commode qui fait que la somme exponentielle $M(\alpha)$ est souvent anormalement petite. Maynard a par exemple démontré que sa norme L^1 vérifie

$$\int_0^1 |M(\alpha)| d\alpha \ll N^{0{,}32},$$

le point essentiel étant que l'exposant 0,32 est même plus petit que $(1-\delta)/2$, ce qui correspond à la compensation optimiste en racine carrée que nous avons mentionnée. De telles estimations permettent d'espérer attaquer le théorème 2. On peut voir l'idée principale de manière transparente dans l'article de Maynard [35], où il démontre une version plus facile du théorème 2 qui traite les nombres premiers auxquels il manque un chiffre en base b, avec b suffisamment grand. L'ensemble des entiers jusqu'à N auxquels il manque un chiffre en base b a une taille d'environ $N^{\log(b-1)/\log b}$. Le problème devient donc plus facile

lorsque la base b devient plus grande. Ramener la base à 10 s'est avéré être un problème d'une difficulté abominable, ce qui est sans doute plus important sur le plan psychologique que pour une quelconque raison mathématique. Maynard [36] s'est attaqué brillamment à ce problème en introduisant un certain nombre d'idées nouvelles, notamment des idées issues de la géométrie des nombres, différents aspects de la théorie des cribles et des comparaisons avec un processus de Markov. On peut s'attendre à ce que, même en base 3, il y ait une infinité de nombres premiers auxquels il manque un chiffre donné. En base 2, le seul chiffre qui pourrait être omis est 0 ; nous nous retrouvons face au problème de savoir s'il y a une infinité de nombres de Mersenne premiers, qui échappe aux mathématiques actuelles. Nous terminons cette discussion en signalant deux autres beaux résultats sur les chiffres des nombres premiers qui ont des éléments en commun avec les travaux de Maynard, à savoir les travaux de Mauduit et Rivat [31] qui montrent notamment que la somme des chiffres décimaux des nombres premiers a la même probabilité d'être paire ou impaire, et les travaux de Bourgain [6] qui permettent de spécifier une petite proportion des chiffres binaires des nombres premiers.

4 Les écarts entre nombres premiers

Nous allons maintenant discuter du résultat le plus spectaculaire de Maynard, le soleil parmi les petites étoiles, à savoir le théorème 1 ci-dessus sur la recherche de nombreux nombres premiers dans des intervalles bornés. Pour décrire l'histoire récente de ce problème, examinons d'abord comment les nombres premiers sont typiquement espacés. Le théorème des nombres premiers nous dit que le n-ième nombre premier p_n vaut environ $n \log n$, de sorte que l'écart moyen entre deux nombres premiers consécutifs, $p_{n+1} - p_n$, est environ $\log p_n$. Quelle est la distribution des écarts normalisés $(p_{n+1} - p_n)/\log p_n$? Le modèle aléatoire de Cramér pour les nombres premiers prédit que ces écarts normalisés devraient se comporter comme un processus de Poisson et que pour tout intervalle fixé $[\alpha, \beta] \in \mathbb{R}_{\geqslant 0}$,

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{ n \leqslant N : \ \frac{p_{n+1} - p_n}{\log p_n} \in [\alpha, \beta] \right\} = \int_\alpha^\beta e^{-t} dt = e^{-\alpha} - e^{-\beta}. \quad (3)$$

Gallagher [16] a montré que cette prédiction découle également des conjectures plus raffinées de Hardy-Littlewood, le point clé étant que

les constantes des séries singulières $\mathfrak{S}(\mathcal{H})$ (voir (1)) valent approximativement 1 (ce qui correspond au modèle naïf de Cramér) en moyenne sur les ensembles $\mathcal{H}$ à k éléments.

Cette conjecture sur les écarts normalisés entre les nombres premiers est très ouverte. En effet, si l'on désigne par $\mathcal{L}$ l'ensemble des points d'accumulation de $(p_{n+1} - p_n)/\log p_n$, alors même l'affirmation qualitative selon laquelle $\mathcal{L} = [0, \infty]$, qui découle immédiatement de (3), est actuellement inconnue. En créant de longues chaînes de nombres composés, Westzynthius a démontré que $\mathcal{L}$ contient ∞, mais pendant longtemps aucun autre point d'accumulation n'était connu bien qu'Erdős et Ricci aient démontré que $\mathcal{L}$ a une mesure de Lebesgue strictement positive. Des progrès spectaculaires ont été accomplis en 2005 grâce aux travaux novateurs de Goldston, Pintz et Yıldırım [17], qui ont démontré que, pour tout $\varepsilon > 0$, il y a une infinité de n tels que $p_{n+1} - p_n \leqslant \varepsilon \log p_n$. Ainsi, les écarts entre les nombres premiers sont faibles par rapport à la moyenne. On sait maintenant que 0 se trouve dans $\mathcal{L}$. Avant les travaux de Goldston, Pintz et Yıldırım, on savait seulement que la différence entre les nombres premiers consécutifs devenait inférieure à environ $\frac{1}{4}$ de l'espacement moyen. Leurs travaux ont ouvert la voie à des avancées ultérieures, notamment au théorème 1 de Maynard.

Supposons que $h_1, \ldots, h_k$ soient des entiers distincts avec $\mathfrak{S}(\{h_1, \ldots, h_k\}) > 0$. De tels k-uplets sont dits *admissibles*. Par exemple, $\{k!, 2 \cdot k!, \ldots, k \cdot k!\}$ est admissible. La conjecture de Hardy-Littlewood prédit qu'il existe une infinité de n avec $n + h_1, \ldots, n + h_k$ tous premiers. Au lieu de vouloir que ces k nombres soient premiers, que se passerait-il si nous demandions seulement qu'au moins deux d'entre eux soient premiers ? Cela montrerait déjà qu'il y a infiniment souvent des écarts bornés entre des nombres premiers consécutifs. Supposons que nous puissions trouver des poids positifs ou nuls $w(n)$ avec la propriété que pour x grand et tout $j = 1, \ldots, k$,

$$\sum_{\substack{x \leqslant n \leqslant 2x \\ n+h_j \text{ premier}}} w(n) > \frac{1}{k} \sum_{x \leqslant n \leqslant 2x} w(n). \tag{4}$$

En additionnant (4) sur tous les $j = 1, \ldots, k$, nous obtiendrions

$$\sum_{x \leqslant n \leqslant 2x} \#\left\{1 \leqslant j \leqslant k : n + h_j \text{ premier}\right\} w(n) > \sum_{x \leqslant n \leqslant 2x} w(n), \tag{5}$$

d'où il découlerait qu'il doit y avoir un certain n avec au moins deux nombres premiers parmi $n + h_1, \ldots, n + h_k$. En considérant les poids

comme une mesure de probabilité sur $x \leqslant n \leqslant 2x$, nous pouvons interpréter (5) comme disant que le nombre attendu de nombres premiers parmi les $n + h_j$ est strictement supérieur à 1, de sorte qu'il doit y avoir des n avec au moins deux nombres premiers dans ce k-uplet.

Le problème difficile est de construire des poids qui vérifient (4). Des choix naturels pour de tels poids sont suggérés par la théorie des cribles, en particulier par la théorie du crible de Selberg. Le choix standard des poids du crible de Selberg (qui sont utilisés pour majorer le nombre de k-uplets premiers $n + h_1, \ldots, n + h_k$) prend la forme

$$w(n) = \left(\sum_{\substack{d \mid (n+h_1)\cdots(n+h_k) \\ d \leqslant \mathrm{R}}} \mu(d) \left(\frac{\log \mathrm{R}/d}{\log \mathrm{R}} \right)^k \right)^2 .$$

Il est clair qu'on a toujours $w(n) \geqslant 0$. En développant la somme, le second membre de (4) (la somme sur tous les $n \in [x, 2x]$) peut être évalué asymptotiquement tant que $\mathrm{R}^2 \leqslant x^{1-\varepsilon}$. Le premier membre de (4) est plus complexe et repose sur la compréhension de la distribution des nombres premiers dans les progressions arithmétiques avec la raison de la progression allant jusqu'à R^2. Le théorème de Bombieri-Vinogradov permet une telle compréhension (à un niveau comparable à celui que donnerait l'hypothèse de Riemann généralisée) tant que $\mathrm{R}^2 \leqslant x^{\frac{1}{2}-\varepsilon}$, de sorte que R est maintenant contraint d'être $\leqslant x^{\frac{1}{4}-\varepsilon}$. Pour ce choix de poids, le nombre attendu de nombres premiers parmi les $n + h_j$ est d'environ $(2k/(k+1)) \log \mathrm{R}/\log x$, de sorte qu'avec $\mathrm{R} \leqslant x^{1/4-\varepsilon}$ on ne s'attend à trouver que $\frac{1}{2}$ nombre premier dans le k-uplet.

Bien que les poids du crible de Selberg décrits ci-dessus aient été optimisés pour les majorants du problème des k-uplets premiers, Goldston, Pintz et Yıldırım ont fait la découverte surprenante qu'il existe de meilleurs choix de poids pour optimiser le rapport des sommes dans (4). Ils ont considéré des poids de la forme

$$w(n) = \left(\sum_{\substack{d \mid (n+h_1)\cdots(n+h_k) \\ d \leqslant \mathrm{R}}} \mu(d) \left(\frac{\log \mathrm{R}/d}{\log \mathrm{R}} \right)^{k+\ell} \right)^2 ,$$

pour un paramètre ℓ convenable, qui s'avère dans le cas optimal être autour de $\sqrt{k}$. Avec ce choix de poids, ils ont constaté que le nombre attendu de nombres premiers parmi les $n + h_j$ est environ deux fois plus

grand qu'auparavant, soit $(4 + O(1/k^{\frac{1}{2}})) \log R/\log x$. Avec $R = x^{\frac{1}{4}-\varepsilon}$, on ne parvient pas à obtenir la relation (4) souhaitée. Cela ne permet donc pas d' établir l'existence d'écarts bornés entre les nombres premiers. En considérant un nombre premier supplémentaire possible $n + h$ pour $1 \leqslant h \leqslant \varepsilon \log x$, Goldston, Pintz, Yıldırım ont pu déduire de cet argument qu'il y a une infinité de n avec $p_{n+1} - p_n \leqslant \varepsilon \log n$. Pour une discussion plus détaillée de ces idées, voir [47].

Si l'on pouvait prendre R comme étant $x^{\frac{1}{4}+\delta}$ avec un $\delta > 0$, alors l'argument de Goldston, Pintz et Yıldırım donnerait des écarts bornés entre les nombres premiers. Pour prendre une telle valeur pour R, il faudrait comprendre la distribution des nombres premiers jusqu'à x dans les progressions arithmétiques lorsque la raison de la progression est aussi grande que $x^{\frac{1}{2}+2\delta}$. Les conjectures d'Elliott-Halberstam prédisent que de tels résultats devraient être valables (en moyenne) lorsque la raison est aussi grande que $x^{1-\varepsilon}$. Des progrès partiels vers de telles extensions du théorème de Bombieri-Vinogradov ont été réalisés par Fouvry et Iwaniec [12] et par Bombieri, Friedlander et Iwaniec [5]. Mais ces résultats ne s'appliquaient pas immédiatement au problème de la démonstration d'écarts bornés entre les nombres premiers. En avril 2013, Yitang Zhang [49] a fait une percée spectaculaire en établissant une version du théorème de Bombieri-Vinogradov dans un intervalle élargi qui était suffisant pour la méthode de Goldston, Pintz et Yıldırım. Zhang a démontré que si $k > 3{,}5\times10^6$, alors pour tout k-uplet admissible $h_1, \ldots, h_k$, il existe une infinité de n pour lesquels au moins deux des $n + h_j$ sont des nombres premiers. Cela implique qu'il y a un nombre infini de cas où l'écart entre deux nombres premiers consécutifs est inférieur à 70 millions. Le projet Polymath [46] a raffiné les travaux de Zhang sur l'équidistribution des nombres premiers dans les progressions arithmétiques. On trouve d'autres raffinements qualitatifs et quantitatifs de ces résultats dans les articles récents de Maynard [37–39].

Les travaux de Zhang ont démontré le cas $m = 2$ du théorème 1. Cependant, même si l'on prenait le plus grand intervalle possible pour R, à savoir $R = x^{\frac{1}{2}-\varepsilon}$ (ce qui serait autorisé par la conjecture d'Elliott-Halberstam), les poids de Goldston-Pintz-Yıldırım montreraient seulement que le nombre attendu de nombres premiers dans un k-uplet admissible est $\geqslant 2 - \varepsilon$. En d'autres termes, même dans le cadre de la conjecture d'Elliott-Halberstam, on ne parviendrait pas à établir l'existence de trois nombres premiers dans des intervalles bornés.

La démonstration du théorème 1 repose sur un choix différent pour les poids $w(n)$, découvert quelques mois seulement après les travaux

de Zhang par Maynard (qui a annoncé les résultats dans un exposé mémorable à Oberwolfach en octobre 2013) et indépendamment par Tao (dans des travaux non publiés). Les poids de Maynard-Tao sont une extension multidimensionnelle des poids considérés précédemment et sont *grosso modo* de la forme

$$w(n) = \left(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i \\ \prod d_i \leqslant \mathrm{R}}} \prod_{i=1}^{k} \mu(d_i)\, \mathrm{F}\left(\frac{\log d_1}{\log \mathrm{R}}, \dots, \frac{\log d_k}{\log \mathrm{R}} \right) \right)^2,$$

avec des fonctions lisses convenables $\mathrm{F} : [0,1]^k \to \mathbb{R}$. De façon surprenante, pour un choix approprié de F, le nombre attendu de nombres premiers parmi $n+h_1, \dots, n+h_k$ (rappelons (5) ci-dessus) est $\geqslant c \log k \frac{\log \mathrm{R}}{\log x}$, avec une constante strictement positive c. En fait, c peut être pris proche de 1 si k est suffisamment grand. Le point clé est que le nombre attendu de nombres premiers dans les k-uplets tende vers l'infini avec k. En fait, il suffit que R croisse comme n'importe quelle puissance de x pour que la méthode réussisse, de sorte que Bombieri-Vinogradov qui permet $\mathrm{R} = x^{\frac{1}{4}-\varepsilon}$ est déjà suffisant ! Ainsi, on a la version plus précise suivante du théorème 1, ce qui peut être considéré comme un résultat partiel vers la conjecture de Hardy-Littlewood sur les k-uplets de nombres premiers.

Théorème 3 (Maynard [32]). *Soit $m \geqslant 2$ un entier naturel. Soit k suffisamment grand par rapport à m. Soit $\mathcal{H} = \{h_1, \dots, h_k\}$ un ensemble de k entiers avec $\mathfrak{S}(\mathcal{H}) > 0$. Il existe alors une infinité de n tels que le k-uplet $n + h_1, \dots, n + h_k$ contienne au moins m nombres premiers.*

Maynard a montré que k peut être pris inférieur à $Cm^2 e^{4m}$ pour une constante C appropriée. D'autres raffinements (qui incorporent également le travail de Zhang) ont été obtenus dans le travail de Baker et Irving [3], qui ont montré qu'on peut prendre pour k la valeur $C\, e^{3,815m}$. Le cas $m = 2$ est particulièrement intéressant : le projet Polymath [45] a optimisé ces arguments pour établir que tout 50-uplet admissible contient deux nombres premiers infiniment souvent. En particulier, ils ont montré que $p_{n+1} - p_n \leqslant 246$ infiniment souvent, et conditionnellement à la conjecture d'Elliott-Halberstam qu'il y a infiniment souvent au moins deux nombres premiers dans le triplet n, $n + 2$, $n + 6$. Mentionnons une autre variante uniforme de ces résultats : Maynard [33]

a montré par exemple qu'il existe au moins $cX\exp\left(-\sqrt{\log X}\right)$ valeurs de $x \in [X, 2X]$ telles que l'intervalle $[x, x + \log X]$ contienne au moins $c \log\log X$ nombres premiers (ici c est une constante strictement positive). Pour des exposés détaillés sur ces résultats de Zhang, Maynard et Tao, voir [18, 29].

Les poids de Maynard-Tao offrent une nouvelle méthode flexible pour étudier de nombreux problèmes sur les nombres premiers et les suites apparentées, et ont trouvé un certain nombre d'applications. Nous décrivons deux autres résultats qui utilisent ces poids, tous deux concernant des écarts entre des nombres premiers consécutifs. Nous avons déjà mentionné le résultat de Westzynthius sur les grands écarts entre nombres premiers consécutifs, qui montrait que ∞ se trouve dans l'ensemble $\mathcal{L}$ des points d'accumulation des écarts normalisés $(p_{n+1} - p_n)/\log p_n$. Ceci a été quantifié dans les années trente par Erdős et Rankin qui ont montré que, pour une constante strictement positive C,

$$\max_{p_n \leqslant X}(p_{n+1} - p_n) \geqslant C \log X \frac{(\log\log X)\log\log\log\log X}{(\log\log\log X)^2}. \tag{6}$$

Le modèle aléatoire suggère que l'écart maximal entre les nombres premiers jusqu'à X devrait être d'environ $(\log X)^2$. C'est ce que l'on appelle la conjecture de Cramér. Bien que cette conjecture soit très délicate, on pense généralement que l'écart maximal ne dépasse pas $(\log X)^{2+\varepsilon}$, bien que même cela dépasse de loin le problème inattaquable de Landau, à savoir l'existence d'un nombre premier entre deux carrés consécutifs. Erdős a attiré l'attention sur le problème de la recherche d'écarts plus grands entre des nombres premiers consécutifs, en offrant 10 000 dollars pour une borne qui remplacerait C dans (6) par une fonction qui tend vers ∞ avec X. Pendant plus de soixante-quinze ans, ce problème a résisté aux attaques, seules des améliorations de la constante C étant connues. Puis, par une coïncidence remarquable, *deux* techniques différentes sont apparues en 2014, qui ont démontré toutes deux l'inégalité (6) avec C remplacé par une fonction qui tend vers l'infini avec X. L'une des approches, celle de Ford, Green, Koniaguine et Tao [11], s'appuyait sur les travaux de Green-Tao sur les progressions arithmétiques de nombres premiers, tandis que l'autre approche, celle de Maynard [34], trouvait un moyen d'adapter les poids du crible de Maynard-Tao. La seconde approche était mieux adaptée pour quantifier les grands écarts qui se produisent. En joignant leurs forces, Ford, Green, Koniaguine, Maynard et Tao [10] ont démontré que, pour une certaine

constante $C > 0$,

$$\max_{p_n \leqslant X}(p_{n+1} - p_n) \geqslant C \log X \frac{(\log\log X)\log\log\log\log X}{\log\log\log X}, \qquad (7)$$

améliorant ainsi l'inégalité (6) par un facteur $\log\log\log X$.

Les résultats sur les petits écarts et les grands écarts entre les nombres premiers consécutifs montrent que 0 et ∞ se trouvent dans l'ensemble $\mathcal{L}$ des points d'accumulation des écarts normalisés des nombres premiers. On ne connaît pas d'autres nombres explicites dans $\mathcal{L}$, bien que l'on s'attende à ce que $\mathcal{L}$ contienne tous les nombres réels positifs ou nuls. Suite à la percée de Zhang, Pintz [42] a montré que $\mathcal{L}$ contient un intervalle $[0, c]$ pour un certain $c > 0$, qui n'est cependant pas effectif et ne peut pas être calculé explicitement. En utilisant les poids du crible de Maynard-Tao, Banks, Freiberg et Maynard [4] ont obtenu le beau résultat suivant : si $\beta_1 \leqslant \beta_2 \leqslant \ldots \leqslant \beta_9$ sont neuf nombres réels quelconques, alors au moins une de leurs différences $\beta_j - \beta_i$ (avec $i < j$) doit être un élément de $\mathcal{L}$. Leur résultat a été affiné par Pintz [43] et Merikoski [41]. Merikoski montre que le même résultat s'applique si nous commençons avec seulement quatre nombres réels $\beta_1 \leqslant \beta_2 \leqslant \beta_3 \leqslant \beta_4$. De plus, Merikoski a également montré que pour tout $T > 0$, l'ensemble $\mathcal{L} \cap [0, T]$ a une mesure d'au moins $T/3$.

5 La conjecture de Duffin-Schaeffer

Nous nous sommes concentrés jusqu'à présent sur les travaux de Maynard relatifs aux nombres premiers. Dans une direction très différente, Maynard a résolu en collaboration avec Koukoulópoulos [28] l'un des problèmes centraux de la théorie métrique de l'approximation diophantienne, connu sous le nom de conjecture de Duffin-Schaeffer.

L'approximation diophantienne consiste à trouver des approximations rationnelles a/q d'un nombre irrationnel donné α, en s'efforçant de rendre $|\alpha - a/q|$ petit par rapport à q. Le résultat le plus fondamental est le théorème de Dirichlet selon lequel pour tout nombre irrationnel α, il existe une infinité d'approximations rationnelles a/q avec $a \in \mathbb{Z}$, $q \in \mathbb{N}$ et $(a, q) = 1$ (de sorte que la fraction soit sous forme réduite) telles que $|\alpha - a/q| \leqslant 1/q^2$. Pour les irrationnels quadratiques comme $\sqrt{2}$ ou le nombre d'or, le théorème de Dirichlet est essentiellement le meilleur possible. Pour tout α de ce type, il existe une constante strictement positive $C(\alpha)$ telle que $|\alpha - a/q| \geqslant C(\alpha)/q^2$ pour toute approximation

rationnelle a/q. Un résultat célèbre de Roth établit que, pour tout irrationnel algébrique α et tout $\varepsilon > 0$, on a $|\alpha - a/q| \geqslant C(\alpha, \varepsilon)/q^{2+\varepsilon}$ avec une constante strictement positive appropriée $C(\alpha, \varepsilon)$. Pour certains nombres transcendants intéressants tels que π, le problème de savoir avec quelle précision on peut les approcher par des nombres rationnels reste ouvert.

L'approximation diophantienne métrique s'intéresse aux problèmes d'approximation qui se posent pour *presque tous* les nombres irrationnels α, où « presque tous » doit être interprété dans le sens de la mesure de Lebesgue. Comme le problème de l'approximation de α par des rationnels est identique à celui de l'approximation de $\alpha + 1$, nous pouvons limiter notre attention aux nombres irrationnels $\alpha \in [0, 1[$. Le problème le plus élémentaire est le suivant : supposons que $\psi : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ soit une fonction donnée, que peut-on dire de la mesure de l'ensemble des $\alpha \in [0, 1[$ pour lesquels il existe une infinité de nombres rationnels a/q sous forme réduite (c'est-à-dire tels que $(a, q) = 1$) avec $|\alpha - a/q| \leqslant \psi(q)$. Le théorème de Dirichlet nous dit par exemple que si $\psi(q) = 1/q^2$, alors tous les nombres irrationnels $\alpha \in [0, 1[$ admettent une infinité de telles approximations rationnelles.

Soit $\mathcal{A}_q = \mathcal{A}_q(\psi)$ l'ensemble des $\alpha \in [0, 1[$ pour lesquels il existe une fraction réduite a/q avec $|\alpha - a/q| \leqslant \psi(q)$, et $\mathcal{A}$ l'ensemble des $\alpha \in [0, 1[$ qui se trouvent dans un nombre infini d'ensembles $\mathcal{A}_q$. Ainsi

$$\mathcal{A} = \bigcap_{Q=1}^{\infty} \widetilde{\mathcal{A}}(Q) \qquad \text{avec} \qquad \widetilde{\mathcal{A}}(Q) = \bigcup_{q=Q}^{\infty} \mathcal{A}_q.$$

La mesure de $\mathcal{A}_q$ est $\leqslant 2\varphi(q)\psi(q)$, puisqu'il y a $\varphi(q)$ choix possibles pour le numérateur a. Si $\psi(q) \leqslant 1/(2q)$, de sorte que les intervalles pour différents a ne se chevauchent pas, alors il y a égalité ici. Si $\sum_{q=1}^{\infty} \varphi(q)\psi(q)$ converge, alors la mesure de $\widetilde{\mathcal{A}}(Q)$ est majorée par $2\sum_{q=Q}^{\infty} \varphi(q)\psi(q)$, qui est le reste d'une série convergente et tend donc vers 0 lorsque $Q \to \infty$. Il s'ensuit que $\mathcal{A}$ a une mesure nulle. Cet argument est identique à la partie facile du théorème de Borel-Cantelli.

Duffin et Schaeffer ont émis en 1941 la conjecture remarquable que dans le cas complémentaire où $\sum_{q=1}^{\infty} \varphi(q)\psi(q)$ diverge, la mesure de $\mathcal{A}$ est 1. Depuis lors, la conjecture de Duffin-Schaeffer est restée l'une des questions centrales de la théorie métrique des approximations diophantiennes. Un certain nombre de résultats partiels pour cette conjecture ont été obtenus. Un beau résultat de Gallagher [15] a par exemple montré que la mesure de l'ensemble $\mathcal{A}(\psi)$ est toujours soit 0

soit 1. Les travaux d'Erdős [9] et de Vaaler [48] ont établi la conjecture lorsque $\psi(q)$ est d'ordre $O(1/q^2)$ pour tout q. Pollington et Vaughan [44] ont démontré des analogues de la conjecture en dimension supérieure. [1,22,23] ont démontré des versions plus faibles de la conjecture avec des conditions de divergence supplémentaires. Mais le problème complet a résisté jusqu'aux travaux récents de Koukoulópoulos et Maynard [28] :

Théorème 4 (Koukoulópoulos et Maynard [28])**.** *Soit $\psi : \mathbb{N} \to \mathbb{R}_{\geqslant 0}$ tel que $\sum_{q=1}^{\infty} \varphi(q)\psi(q)$ diverge. Alors l'ensemble des $\alpha \in [0,1]$ qui ont une infinité d'approximations rationnelles $|\alpha - a/q| \leqslant \psi(q)$ avec $(a,q) = 1$ a une mesure de Lebesgue égale à 1. En d'autres termes, la conjecture de Duffin-Schaeffer est vérifiée.*

Nous renvoyons à l'exposé de Koukoulópoulos au congrès international des mathématiciens [27] pour une présentation plus détaillée de ce résultat et des idées qui sous-tendent sa démonstration.

Nous avons donné un aperçu de certains des travaux les plus spectaculaires de Maynard dans le domaine de la théorie analytique des nombres. Le travail de Maynard se caractérise par des idées ingénieuses mais simples, qui sont poussées très loin grâce à ses puissantes capacités techniques. Aussi impressionnant qu'ait été son travail jusqu'à présent, il ne marque peut-être qu'un début.

Financement. Ce travail a été partiellement soutenu par des subventions de la Fondation nationale des sciences et par une bourse de la fondation Simons.

Bibliographie

[1] *Adv. Math.*, n° 356, 2019, article 106808.
[2] *Proc. Lond. Math. Soc.*, n° 83, 2001, p. 532-562.
[3] *Math. Z.*, n° 286, 2017, p. 821-841.
[4] *Proc. Lond. Math. Soc.*, n° 113, 2016, p. 515-539.
[5] *Acta Math.*, n° 156, 1986, p. 203-251.
[6] *Israel J. Math.*, n° 206, 2015, p. 165-182.
[7] *J. Number Theory*, n° 81 , 2000, p. 270-291.
[8] *J. Number Theory*, n° 91, 2001, p. 230-255.
[9] *J. Number Theory*, n° 2, 1970, p. 425-441.
[10] *J. Am. Math. Soc.*, n° 31, 2018, p. 65-105.
[11] *Ann. Math.*, n° 183, 2016, p. 935-974.
[12] *Mathematika*, n° 27, 1980, p. 135-152.

[13] *Ann. Math.*, nº 148, 1998, p. 945-1040.

[14] Friedlander (John) et Iwaniec (Henryk), *Opera de cribro*, American Mathematical Society, 2010.

[15] *J. Math. Soc. Japan* , nº 13, 1961, p. 342-345.

[16] *Mathematika*, nº 23, 1976, p. 4-9.

[17] *Ann. Math.*, nº 170, 2009, p. 819-862.

[18] *Bull. Am. Math. Soc. (N.S.)*, nº 52, 2015, p. 171-222.

[19] *Ann. Math.* , nº 171, 2010, p. 1753-1850.

[20] *Ann. Math.*, nº 175, 2012, p. 541-566.

[21] *Ann. Math.*, nº 176, 2012, p. 1231-1372.

[22] Harman (Glyn), *Metric Number Theory*, Oxford University Press, 1998.

[23] *Math. Ann.*, nº 353, 2012, p. 259-273.

[24] *Acta Math.* , nº 186, 2001, p. 1-84.

[25] *Invent. math.*, nº 208, 2017, p. 441-499.

[26] *Proceedings of the International Congress of Mathematicians (Seoul, 2014)*, vol. II, p. 391-418.

[27] arXiv, 2109.11003.

[28] *Ann. Math.*, nº 192, 2020, p. 251-307.

[29] *Astérisque*, nº 367-368, 2015, p. 327-366.

[30] *Proc. Lond. Math. Soc.*, nº 115, 2017, p. 323-347.

[31] *Ann. Math.*, nº 171, 2010, p. 1591-1646.

[32] *Ann. Math.*, nº 181 , 2015, p. 383-413.

[33] *Compos. Math.* , nº 152, 2016, p. 1517-1554.

[34] *Ann. Math.*, nº 183 , 2016, p. 915-933.

[35] *European Congress of Mathematics (Berlin, 2016)*, EMS Press, 2018, p. 641-661.

[36] *Invent. math.*, nº 217 , 2019, p. 127-218.

[37] arXiv, 2006.06572.

[38] arXiv, 2006.07088.

[39] arXiv, 2006.08250.

[40] *Forum Math. Pi* , nº 8, 2020, article e3.

[41] *J. Lond. Math. Soc.*, nº 102, 2020, p. 99-124.

[42] *From Arithmetic to Zeta-Functions*, Springer, 2016, p. 367-384.

[43] *Acta Arith.*, nº 184, 2018, p. 413-418.

[44] *Mathematika*, nº 37, 1990, p. 190-200.

[45] *Algebr. Number Theory*, nº 8, 2014, p. 2067-2199.

[46] *Res. Math. Sci.*, nº 1, 2014, article 12.

[47] *Bull. Am. Math. Soc.* , nº 44, 2007, p. 1-18.

[48] *Pacific J. Math.*, nº 76, 1978, p. 527-539.

[49] *Ann. Math.*, nº 179 , 2014, p. 1121-1174.

Les travaux de Maryna Viazovska (par Henry Cohn)

Le 5 juillet 2022, Maryna Viazovska a reçu une médaille Fields pour la résolution du problème de l'empilement de sphères en dimension 8, ainsi que pour d'autres contributions à des problèmes extrémaux connexes et à des problèmes d'interpolation en analyse harmonique. Cet article explique à un public mathématicien certaines des idées qui sous-tendent ses travaux.

1 Introduction

Le problème de l'empilement de sphères consiste à déterminer comment remplir la fraction la plus grande possible de l'espace avec des sphères semblables, si elles ne peuvent se toucher que tangentiellement [1]. Ce problème se situe à l'interface de nombreuses branches des mathématiques et de la science en général, avec des liens allant de la science des matériaux à la théorie de l'information. L'empilement de sphères est un problème naturel de géométrie euclidienne, dont l'énoncé est simple. On pourrait s'attendre à une solution tout aussi élémentaire et autonome. Au lieu de cela, le sujet est dominé par des liens inattendus.

Avant les travaux révolutionnaires de Viazovska, la densité optimale d'empilement de sphères n'était connue qu'en dimension 1, 2 ou 3. En dimension 1, c'est trivial, car les intervalles peuvent recouvrir la droite réelle avec une densité égale à 1. En dimension 2, ce n'est pas trivial, mais Thue [26] a démontré que l'arrangement de six voisins autour de chaque disque est optimal, avec une densité $\pi/\sqrt{12} \approx 0{,}9068$. Le cas de la dimension 3 a été résolu par Hales [16] *via* une démonstration ingénieuse assistée par ordinateur, qui a depuis été formellement vérifiée [17]. La réponse sans surprise est illustrée dans la figure 1 : les

Cohn (Henry), « The work of Maryna Viazovska », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 82-105. DOI 10.4171/ICM2022/213

1. Pour énoncer le problème avec précision, il faut expliquer ce que signifie « la fraction la plus grande possible ». Une façon de le faire est de prendre une limite du problème de l'empilement dans une région délimitée lorsque sa taille augmente par rapport au rayon de la sphère. Le problème de l'empilement de sphères s'avère être très robuste, dans le sens où à peu près toutes les formulations raisonnables sont équivalentes.

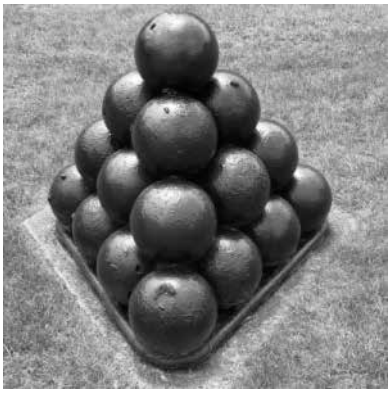


Fig. 1 – *Un empilement optimal de boulets de canon.*

couches bidimensionnelles optimales sont imbriquées les unes dans les autres aussi densément que possible, pour atteindre la densité $\pi/\sqrt{18} \approx 0{,}7404$.

Ces résultats antérieurs donnent une image trompeuse de ce qui se passe dans les dimensions supérieures. L'empilement de couches optimales pour la dimension inférieure produit généralement des empilements sous-optimaux. Personne n'a la moindre idée de ce que pourraient être les empilements de sphères les plus denses dans la plupart des dimensions. Nous ne savons même pas s'ils doivent être cristallins ou désordonnés.

Les empilements en dimensions supérieures ne présentent pas seulement un intérêt en mathématiques pures. Ils sont également importants pour les applications pratiques, car les empilements de sphères sont des codes correcteurs pour un canal de communication continu (tel que la radio). Dans ce modèle, l'empilement se fait dans un espace de signal abstrait, dont la dimension est le nombre de mesures utilisées pour caractériser le signal ; elle est généralement beaucoup plus grande que trois.

Il ne semble pas y avoir de motif simple dans les empilements optimaux qui persiste pour de nombreuses dimensions. Les meilleures majorations et minorations connues pour la densité optimale d'empilement dans $\mathbb{R}^d$ restent exponentiellement éloignées les unes des autres lorsque d augmente. Une poignée de dimensions sortent néanmoins du lot, notamment les dimensions 8 et 24 qui présentent des empilements exceptionnels, à savoir le réseau E_8 et le réseau de Leech Λ_{24}, avec des symétries remarquables et de nombreux liens avec différentes branches

des mathématiques. Grâce aux travaux de Viazovska [10, 27], nous savons maintenant qu'ils sont véritablement optimaux. Le saut de la dimension 3 aux dimensions 8 et 24 dans les solutions connues est remarquable. Il illustre le caractère exceptionnel de ces empilements.

Le réseau E_8 et le réseau de Leech ont longtemps été considérés comme les candidats les plus convaincants pour trouver de nouvelles solutions au problème de l'empilement de sphères. Une démonstration géométrique directe semblait cependant impossible : il est naturel d'essayer de travailler avec une décomposition de l'espace en mailles, mais le fléau de la dimension signifie que nous sommes confrontés à un nombre ingérable de formes de mailles potentielles et de façons dont elles pourraient s'adjoindre les unes aux autres. Il existe peut-être une démonstration dans ce sens, mais personne n'a encore trouvé la bonne approche.

Au lieu de cela, Viazovska a démontré l'optimalité de E_8 grâce à un nouveau lien spectaculaire avec la théorie des formes modulaires, puis elle a étendu ses idées avec plusieurs collaborateurs au cas du réseau de Leech :

Théorème 5 (Viazovska [27])**.** *Le réseau* E_8 *atteint la densité optimale d'empilement de sphères dans* $\mathbb{R}^8$*, à savoir* $\pi^4/384$*.*

Théorème 6 (Cohn, Kumar, Miller, Radchenko et Viazovska [10])**.** *Le réseau de Leech* Λ_{24} *atteint la densité optimale d'empilement dans* $\mathbb{R}^{24}$*, à savoir* $\pi^{12}/12!$*.*

Comme Peter Sarnak l'a remarqué à l'époque [19], l'article [27] est « étonnamment simple, comme le sont toutes les grandes choses ». Cette simplicité est caractéristique du travail de Viazovska : elle a le don de relier les concepts et de formuler des conjectures audacieuses. Ses idées la conduisent à des arguments saisissants. Ses démonstrations s'attaquent directement au cœur du problème, sans aucune complication extérieure. Bien entendu, la simplicité n'est pas synonyme de facilité. Ce qui rend son travail extraordinaire, c'est à quel point ses idées sont différentes de celles qui ont précédé.

Dans la suite de cet article, nous examinerons la démonstration de Viazovska de l'optimalité de E_8, ainsi que sa motivation et sa place dans les mathématiques de manière plus générale. En particulier, cet article peut servir d'introduction et de guide aux techniques de Viazovska, à côté d'autres exposés [6, 20]. Pour le contexte sur l'empilement de sphères et sur les réseaux, voir [12, 15, 25].

Bien sûr, nous devons garder à l'esprit que ce sujet ne représente qu'un volet des recherches de Viazovska. Par exemple, [3] est un article magnifique et décisif sur un sujet tout à fait différent. Pour quels travaux sera-t-elle connue dans vingt ou trente ans ? J'ai hâte de le découvrir.

2 Le contexte

Avant d'aborder la démonstration de Viazovska, nous avons besoin d'un peu de contexte. Dans cette section, nous allons construire le réseau E_8 et expliquer une méthode pour démontrer des majorations pour la densité d'empilement de sphères.

Les empilements de sphères peuvent être construits de nombreuses façons, parmi lesquelles les empilements en réseau constituent la possibilité la plus simple. Un empilement de sphères est centré sur les points d'un *réseau* Λ dans $\mathbb{R}^d$, c'est-à-dire un sous-groupe discret de $\mathbb{R}^d$ de rang d, ou de manière équivalente un sous-groupe discret engendré par une base de $\mathbb{R}^d$. Il n'y a aucune raison *a priori* pour qu'un empilement optimal de sphères ait cette structure algébrique. Par exemple, le meilleur empilement de sphères connu dans $\mathbb{R}^{10}$ ne l'a pas. Plusieurs des meilleurs empilements de sphères connus en basse dimension sont néanmoins des empilements en réseau.

Pour former un empilement à partir d'un réseau Λ, nous devons choisir le rayon de la sphère r de manière à ce que les sphères voisines ne se chevauchent pas. Plus précisément, nous devons prendre

$$r = \tfrac{1}{2} \min_{x \in \Lambda \setminus \{0\}} |x|.$$

Le volume d'une sphère de rayon r dans $\mathbb{R}^d$ est $\pi^{d/2} r^n / (d/2)!$, où $(d/2)!$ signifie $\Gamma(d/2+1)$ lorsque d est impair. La *densité* de l'empilement global (c'est-à-dire la fraction d'espace couverte par les boules) est le volume de la sphère multiplié par le nombre de sphères par unité de volume dans l'espace. Soit $\mathrm{vol}\big(\mathbb{R}^d/\Lambda\big)$ le *covolume* du réseau, c'est-à-dire le volume du tore quotient, ou de manière équivalente la valeur absolue du déterminant d'une base du réseau. Le nombre de sphères par unité de volume dans l'espace est alors de $1/\mathrm{vol}\big(\mathbb{R}^d/\Lambda\big)$. La densité de l'empilement en réseau est donc

$$\frac{\pi^{d/2}\, r^n}{(d/2)!\ \mathrm{vol}\big(\mathbb{R}^d/\Lambda\big)}.$$

L'un des réseaux les plus remarquables est le réseau E_8, qui trouve son origine dans la théorie de Lie mais qui s'est depuis répandu dans toutes les mathématiques. Nous verrons ci-dessous comment obtenir E_8 en modifiant le réseau D_d, le réseau en damier en dimension d défini par

$$D_d = \left\{(x_1, \dots, x_d) \in \mathbb{Z}^d : x_1 + \cdots + x_d \text{ est pair}\right\}.$$

En d'autres termes, D_d omet simplement un point sur deux dans le réseau cubique $\mathbb{Z}^d$. Comme cas particulier, D_3 est le réseau cubique à faces centrées en dimension 3, pour lequel Hales a montré qu'il atteignait la densité optimale d'empilement de sphères [16]. Les réseaux D_4 et D_5 sont les meilleurs empilements connus dans leurs dimensions respectives, mais D_d n'est pas optimal au-delà de la dimension 5.

Le problème de D_d en dimensions supérieures est que ses trous sont trop grands. Un *trou* est un point de l'espace qui est un maximum local pour la distance au réseau. Il existe deux types de trous dans D_d : les trous peu profonds à une distance 1 du réseau tels que $(1, 0, \dots, 0)$, et les trous profonds à une distance $\sqrt{d/4}$ du réseau tels que $(\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2})$. Lorsque $d \to \infty$, $\sqrt{d/4}$ fait de même : les trous profonds deviennent suffisamment grands pour accueillir un très grand nombre de sphères supplémentaires. En particulier, D_d ne peut pas être optimal lorsque d est grand.

Lorsque $d = 8$, quelque chose de magnifique se produit. La distance $\sqrt{8/4}$ entre un trou profond et le réseau est exactement égale à la distance $\sqrt{2}$ entre les points du réseau dans D_8, ce qui signifie que les trous profonds sont juste assez grands pour être remplis par des sphères supplémentaires. Si nous bouchons ces trous avec des sphères, alors l'empilement qui en résulte est l'union de D_8 et de son translaté $D_8 + (\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2})$. Il n'est pas difficile de vérifier que cet empilement est un réseau (cela revient à dire que $2 \cdot (\frac{1}{2}, \frac{1}{2}, \dots, \frac{1}{2}) \in D_8$), appelé « réseau E_8 ».

Le réseau E_8 a un rayon $r = \sqrt{2}/2$ et un covolume $\mathrm{vol}\left(\mathbb{R}^8/E_8\right) = \mathrm{vol}\left(\mathbb{R}^8/D_8\right)/2 = 1$. Il a donc une densité égale à $\pi^4/384 \approx 0{,}2536$. Il n'est pas du tout évident que cette construction soit optimale. En fait, elle semble un peu *ad hoc*. Le réseau E_8 s'avère cependant être bien plus beau et symétrique que sa construction ne l'indique (voir par exemple la figure 2 pour une vue de E_8 avec une symétrie d'ordre 30). Il s'agit d'un cas courant avec les structures exceptionnelles en mathématiques : elles sont généralement obtenues en assemblant plusieurs sous-structures

qui ont chacune moins de symétrie individuellement.

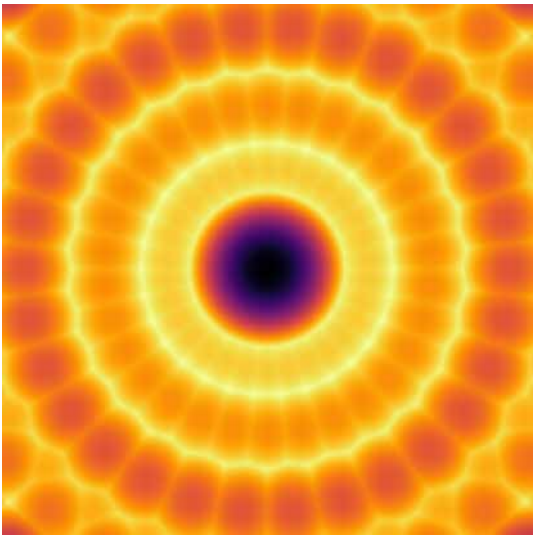


FIG. 2 – *Coupe bidimensionnelle de* $\mathbb{R}^8$ *à travers un plan de Coxeter de* E_8*, colorée en fonction du carré de la distance au point de* E_8 *le plus proche (les couleurs sombres sont les plus proches) et inspirée de [22].*

Maintenant que nous disposons du réseau E_8, la question suivante est de savoir comment nous pourrions essayer d'obtenir un majorant pour la densité d'empilement de sphères en dimension 8. L'obtention d'un majorant semble totalement infaisable dans la plupart des dimensions. Mais dans quelques dimensions spéciales, les majorants basés sur l'analyse harmonique fonctionnent remarquablement bien. Cette idée, appelée « borne de programmation linéaire », remonte à un article fondamental de P. Delsarte [13] sur les codes correcteurs. La borne correspondante pour les empilements de sphères a été développée par Cohn et Elkies [7].

La borne de programmation linéaire est formulée en utilisant la transformée de Fourier $\widehat{f}$ d'une fonction intégrable $f\colon \mathbb{R}^d \to \mathbb{C}$,

$$\widehat{f}(y) = \int_{\mathbb{R}^d} f(x)\, e^{-2\pi i \langle x,y\rangle}\, dx,$$

où $\langle \cdot, \cdot \rangle$ est le produit scalaire habituel sur $\mathbb{R}^d$. Rappelons que la transfor-

mée de Fourier décompose f en exponentielles complexes. En termes de traitement du signal, cela revient à identifier les fréquences qui apparaissent dans un signal et leurs amplitudes relatives. Cette décomposition conduit au *théorème d'inversion de Fourier* : si $\widehat{f}$ est également intégrable, alors

$$f(x) = \int_{\mathbb{R}^d} \widehat{f}(y)\, e^{2\pi i \langle x,y \rangle}\, dy.$$

En d'autres termes, la transformée de Fourier est presque son propre inverse, le changement de signe étant la seule différence. Notons que $\widehat{f}$ est généralement à valeurs complexes même si f est à valeurs réelles. Mais $\widehat{f}$ est à valeurs réelles si f est à valeurs réelles et si c'est une fonction paire.

Nous aurons également besoin de quelques types de fonctions qui se comportent bien. Une fonction $f\colon \mathbb{R}^d \to \mathbb{R}$ est dite « à décroissance rapide » si $f(x) = \mathrm{O}\left(|x|^{-c}\right)$ quand $|x| \to \infty$ pour toute constante $c > 0$. Une *fonction de Schwartz* est une fonction lisse à décroissance rapide dont toutes les dérivées partielles (de tous les ordres) sont également à décroissance rapide. Les fonctions de Schwartz sont sans doute les fonctions avec le meilleur comportement en analyse harmonique. Une grande partie de ce que nous allons aborder peut être généralisée au-delà des fonctions de Schwartz, mais c'est tout ce dont Viazovska a eu besoin pour résoudre le problème de l'empilement de sphères.

Nous pouvons maintenant énoncer la borne de programmation linéaire pour l'empilement de sphères :

Théorème 7 (Cohn et Elkies [7]). *Soit $f\colon \mathbb{R}^d \to \mathbb{R}$ une fonction de Schwartz paire et r un nombre réel strictement positif. Si*

1. $f(x) \leqslant 0$ *pour tout* $x \in \mathbb{R}^d$ *tel que* $|x| \geqslant r$,
2. $\widehat{f}(y) \geqslant 0$ *pour tout* $y \in \mathbb{R}^d$,
3. $f(0) = \widehat{f}(0) = 1$,

alors la densité optimale d'empilement de sphères dans $\mathbb{R}^d$ est inférieure ou égale à $\mathrm{vol}\left(\mathrm{B}^d_{r/2}\right) = \pi^{d/2}(r/2)^d/(d/2)!$.

Ce théorème donne un majorant pour la densité optimale d'empilement à partir d'une fonction f qui vérifie certaines inégalités, mais il ne dit rien sur la façon de choisir f pour optimiser la borne. L'optimisation numérique peut produire de bons choix pour f, qui donnent les bornes indiquées dans la figure 3. Ces bornes sont rigoureuses, mais

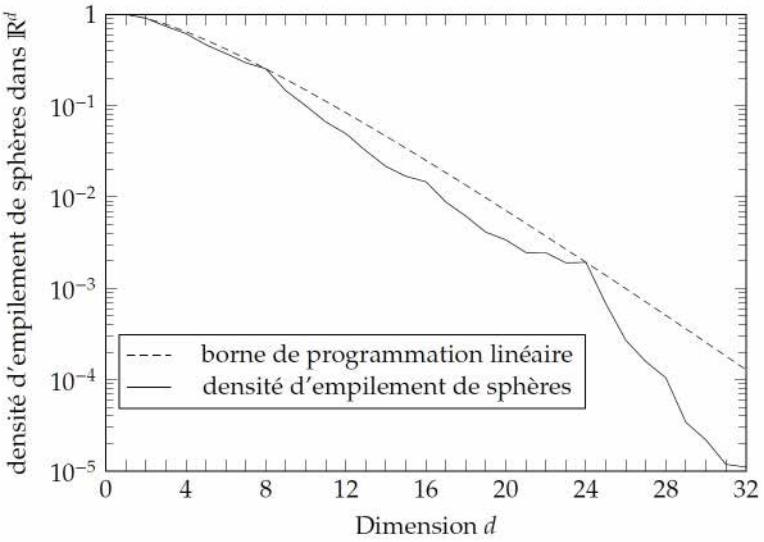


FIG. 3 – *Graphes de la borne de programmation linéaire calculée numériquement [1] et de la meilleure densité d'empilement de sphères actuellement connue [12].*

il est possible que d'autres fonctions produisent des bornes encore meilleures.

Comme on peut le voir sur la figure 3, les bornes en dimension 8 et 24 semblent optimales. L'optimisation numérique ne permettra pas d'obtenir une borne exactement optimale, mais elle semble s'en approcher le plus possible. Sur la base de données de ce type et d'analogies avec d'autres problèmes de la théorie des codes, Cohn et Elkies ont conjecturé l'existence de *fonctions magiques* f qui résoudraient le problème de l'empilement de sphères de manière exacte dans $\mathbb{R}^8$ et $\mathbb{R}^{24}$, avec respectivement $r = \sqrt{2}$ et $r = 2$. Notons que ce n'est pas parce que la borne est plus basse dans ces dimensions, mais plutôt parce que les empilements optimaux l'atteignent. Aucune autre dimension supérieure à 2 ne semble avoir une borne de programmation linéaire optimale, mais aucune démonstration n'existe à ce sujet. La borne n'a été optimisée de manière exacte que pour $d = 1$, 8 et 24.

Le cœur de la percée de Viazovska réside dans la construction de fonctions magiques. À quoi doit ressembler f si l'on veut obtenir une borne optimale ? Il existe quelques critères simples, que nous pouvons

obtenir à partir de la démonstration du théorème 7. Nous examinerons une démonstration pour le cas particulier des réseaux, mais le théorème peut être démontré dans toute sa généralité en combinant la même technique avec un peu d'algèbre supplémentaire. L'argument est basé sur la *formule sommatoire de Poisson* : si $f\colon \mathbb{R}^d \to \mathbb{C}$ est une fonction de Schwartz, si Λ est un réseau dans $\mathbb{R}^d$, et si Λ^* est son *réseau dual* (c'est à dire le réseau engendré par la base duale de toute base de Λ par rapport au produit scalaire $\langle \cdot, \cdot \rangle$), alors

$$\sum_{x\in\Lambda} f(x) = \frac{1}{\operatorname{vol}\left(\mathbb{R}^d/\Lambda\right)} \sum_{y\in\Lambda^*} \widehat{f}(y).$$

Démonstration du théorème 7 pour les réseaux. Le problème de l'empilement de sphères est invariant par changement d'échelle. Nous pouvons donc utiliser des sphères de rayon $r/2$. Soit Λ un empilement en réseau avec un rayon d'empilement $r/2$, ce qui signifie que $|x| \geqslant r$ pour $x \in \Lambda \setminus \{0\}$. Si f vérifie les hypothèses du théorème 7, alors $f(x) \leqslant 0$ pour $x \in \Lambda \setminus \{0\}$ et $\widehat{f}(y) \geqslant 0$ pour tout y, d'où il découle que

$$1 = f(0) \geqslant \sum_{x\in\Lambda} f(x) = \frac{1}{\operatorname{vol}\left(\mathbb{R}^d/\Lambda\right)} \sum_{y\in\Lambda^*} \widehat{f}(y) \geqslant \frac{\widehat{f}(0)}{\operatorname{vol}\left(\mathbb{R}^d/\Lambda\right)} = \frac{1}{\operatorname{vol}\left(\mathbb{R}^d/\Lambda\right)}.$$

Par conséquent, la densité d'empilement $\operatorname{vol}\left(\mathrm{B}^d_{r/2}\right)/\operatorname{vol}\left(\mathbb{R}^d/\Lambda\right)$ est majorée par $\operatorname{vol}\left(\mathrm{B}^d_{r/2}\right)$, comme souhaité. □

Une première observation est que nous pouvons supposer sans perte de généralité que la fonction f est radiale, c'est-à-dire que $f(x)$ ne dépend que de $|x|$. En effet, nous pouvons remplacer f par la moyenne de ses rotations autour de l'origine, car toutes les contraintes sont linéaires et invariantes par rapport à la rotation. On pourrait se demander si les fonctions non radiales pourraient être utiles d'un point de vue conceptuel même si elles ne sont pas nécessaires, mais la réponse semble jusqu'à présent négative. Les travaux de Viazovska conduisent au contraire à une merveilleuse et nouvelle théorie de l'interpolation pour les fonctions radiales. Nous supposerons dorénavant que la fonction f est radiale. Pour tout $t \in [0, \infty[$, nous noterons $f(t)$ la valeur commune de $f(x)$ pour $|x| = t$ et $f'(t)$ la dérivée radiale.

Si nous examinons maintenant l'inégalité centrale dans la démonstration du théorème 7 pour les réseaux, nous pouvons voir quand elle

pourrait être optimale. Pour obtenir une borne optimale, tous les termes écartés de l'inégalité doivent s'annuler : nous devons avoir $f(x) = 0$ pour tout $x \in \Lambda \setminus \{0\}$ et $\widehat{f}(y) = 0$ pour tout $y \in \Lambda^* \setminus \{0\}$. En d'autres termes, f doit s'annuler pour les distances non nulles sur les points du réseau, tandis que $\widehat{f}$ doit s'annuler pour les distances non nulles sur les points du réseau dual.

On peut vérifier directement à partir de la construction de E_8 donnée ci-dessus que $E_8^* = E_8$ et que les longueurs des vecteurs dans E_8 sont toutes des racines carrées d'entiers pairs. De plus, il s'avère que chaque distance $\sqrt{2n}$ avec $n \geqslant 0$ se trouve effectivement dans E_8. Nous devrions donc avoir $r = \sqrt{2}$ dans le théorème 7. La fonction magique f devrait changer de signe au rayon $\sqrt{2}$, avec des racines doubles en $\sqrt{2n}$ pour $n \geqslant 2$, comme indiqué dans la figure 4. En d'autres termes, nous souhaitons contrôler le comportement de f et de $\widehat{f}$ au second ordre en ces points, c'est-à-dire contrôler à la fois les valeurs $f\left(\sqrt{2n}\right)$ et $\widehat{f}\left(\sqrt{2n}\right)$ et les dérivées radiales $f'\left(\sqrt{2n}\right)$ et $\widehat{f}'\left(\sqrt{2n}\right)$.

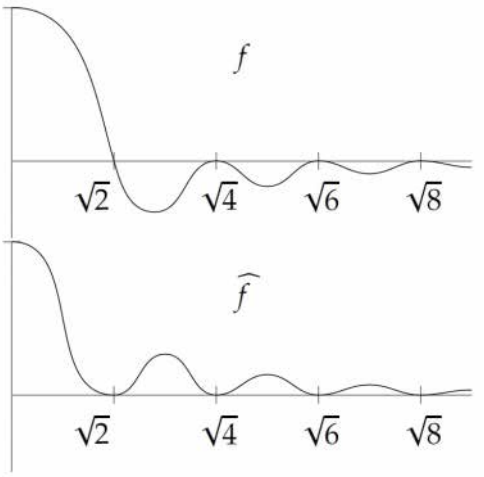


FIG. 4 – *Ce schéma, tiré de [6], présente les racines de la fonction magique f et de sa transformée de Fourier $\widehat{f}$ en dimension 8. Il ne s'agit pas du véritable tracé de la fonction, qui décroît très rapidement. Voir la figure 5 pour le véritable tracé.*

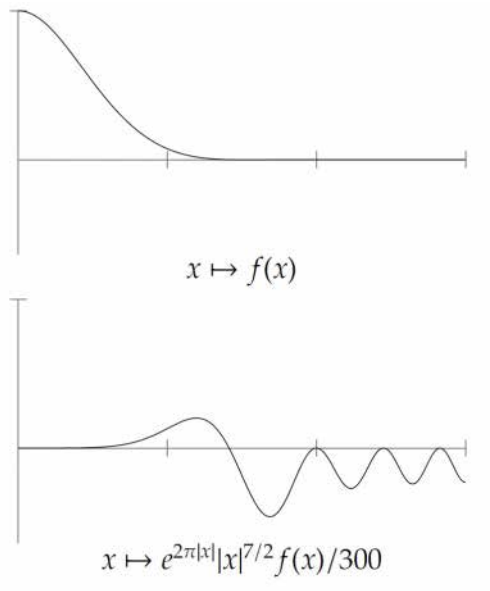


FIG. 5 – *Deux tracés de la fonction magique de Viazovska en dimension 8. L'échelle du premier tracé est correcte, mais la décroissance est si rapide que les racines deviennent invisibles. Le second tracé introduit un changement d'échelle pour les rendre visibles, basé sur le taux de décroissance asymptotique.*

Comment peut-on construire une telle fonction f ? La raison pour laquelle cette tâche est difficile est qu'elle implique de contrôler simultanément f et $\widehat{f}$. Il est bien sûr facile de contrôler l'une ou l'autre de ces fonctions, mais le fait de les contrôler toutes les deux en même temps introduit de profondes difficultés. Le problème sous-jacent est le principe d'incertitude de Heisenberg : en termes simples, chaque fois que vous essayez de fixer f, vous perdez le contrôle de $\widehat{f}$, et *vice versa*. Plus précisément, nous nous heurtons au principe d'incertitude de Bourgain, Clozel et Kahane pour le contrôle des signes des fonctions [4, 8]. Ces inégalités apparemment simples sur f et $\widehat{f}$ se révèlent donc beaucoup plus subtiles qu'il n'y paraît.

Lorsque Elkies et moi-même avons proposé cette méthode en 1999, Viazovska était encore au lycée. Sans réaliser à quel point l'étape restante était profondément difficile, j'ai imaginé que nous avions presque

résolu le problème de l'empilement de sphères pour les dimensions 8 et 24. Notre incapacité à trouver les fonctions magiques était extrêmement frustrante. Je craignais au début que quelqu'un d'autre ne trouvât une solution facile et que je me sentisse idiot de ne pas l'avoir trouvée moi-même. Au fil du temps, j'ai acquis la conviction que l'obtention de ces fonctions était en fait difficile. D'autres personnes sont parvenues à la même conclusion. Thomas Hales a par exemple déclaré : « J'avais l'impression qu'il faudrait un Ramanujan pour la trouver » [19]. Finalement, au lieu de m'inquiéter que quelqu'un d'autre résolve le problème, j'ai commencé à craindre que personne ne le résolve et que je meure un jour sans en connaître le résultat. Je suis reconnaissant à Viazovska d'avoir trouvé une solution aussi satisfaisante et belle, et d'avoir introduit de nouvelles idées merveilleuses à explorer par la communauté mathématique.

3 Les formes modulaires

La fonction magique de Viazovska est construite à l'aide de formes modulaires, des fonctions spéciales qui jouent un rôle important en théorie des nombres. La théorie des formes modulaires a la réputation d'être quelque peu rébarbative, mais les bases ne sont pas si difficiles. Or c'est tout ce qui est nécessaire pour la démonstration de Viazovska. Nous décrirons ici les grandes lignes de la théorie nécessaire. Pour une introduction concrète au cas de $\mathrm{SL}_2(\mathbb{Z})$, voir le chapitre VII dans [24]. Pour des traitements plus détaillés et plus généraux, voir [5, 14, 28].

Nous commençons par un exemple de forme modulaire, à savoir la série d'Eisenstein. Rappelons que la fonction zêta de Riemann est définie par

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

lorsque cette somme converge, c'est-à-dire lorsque $\mathrm{Re}(s) > 1$. Nous additionnons ici les puissances inverses de la progression arithmétique 1, 2... Euler a obtenu une formule exacte lorsque s est un entier pair. Et si nous voulions additionner les puissances inverses d'un réseau dans le plan complexe ? En mettant de côté la question de savoir pourquoi nous voudrions faire cela (le résultat a une signification plus profonde qu'on ne pourrait le supposer), nous pourrions écrire le résultat sous la

forme de la *série d'Eisenstein*

$$\mathrm{E}_k(z) = \frac{1}{2\,\zeta(k)} \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(mz+n)^k} \tag{1}$$

pour $\operatorname{Im} z > 0$, où l'on fait la somme sur le réseau $\{mz + n : m, n \in \mathbb{Z}\}$, à l'exception du point $(0, 0)$ où la somme exploserait. À multiplication par un nombre complexe près, tous les réseaux bidimensionnels sont de cette forme.

Le facteur $1/(2\zeta(k))$ dans la définition est simplement un facteur de normalisation pratique, qui ne joue aucun rôle essentiel dans l'étude de E_k. La notation E_k est malheureusement en conflit avec le nom du réseau E_8, mais cela ne causera pas d'ambiguïté en pratique.

Nous limiterons notre attention aux entiers k strictement positifs pour que $(mz + n)^k$ soit univoque. La série (1) converge absolument lorsque $k \geqslant 3$, mais n'est que semi-convergente lorsque $k = 2$. Pour k impair, les termes (m, n) et $(-m, -n)$ s'annulent et nous obtenons $\mathrm{E}_k(z) = 0$. Donc seuls les cas pairs sont intéressants [2]. Nous nous concentrerons donc sur E_k pour k pair et au moins égal à 4.

À quoi ressemble une série d'Eisenstein ? La figure 6 représente E_4 : le noir représente zéro, le blanc l'infini et la couleur indique la phase complexe [21], les transitions nettes de couleur se produisant pour des valeurs réelles strictement positives. La structure fractale visible dans cette figure peut être expliquée à l'aide de deux équations fonctionnelles :

$$\mathrm{E}_k(z+1) = \mathrm{E}_k(z) \quad \text{et} \quad \mathrm{E}_k(-1/z) = z^k \mathrm{E}_k(z).$$

Ces symétries découlent du réarrangement de la série (1) lorsque $k > 2$. Ce sont les équations centrales de la théorie des formes modulaires.

Les applications $z \mapsto z + 1$ et $z \mapsto -1/z$ qui apparaissent dans ces équations fonctionnelles engendrent un groupe discret de transformations homographiques du *demi-plan supérieur* $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$. Pour le situer dans le contexte plus large des groupes de matrices, nous pouvons considérer l'action de la matrice $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ sur $\mathcal{H}$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}.$$

2. Ce phénomène de parité est essentiellement le même que dans la formule d'Euler pour la fonction zêta aux entiers pairs, qui peut être vue comme le calcul explicite de $\sum_{n\in\in Z\setminus\{0\}} n^{-k}$ pour tous les entiers $k > 1$.

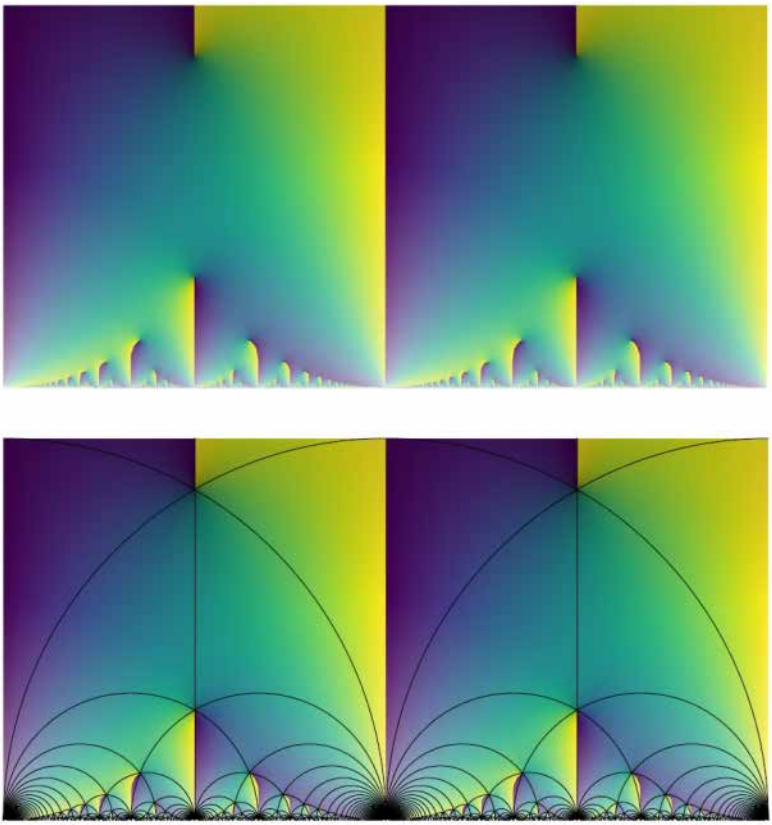


FIG. 6 – *Tracé de la série d'Eisenstein* $\mathrm{E}_4(z)$ *pour* $-1 \leqslant \mathrm{Re}\, z \leqslant 1$ *et* $0 < \mathrm{Im}\, z \leqslant 1$ *(en haut) et le même tracé superposé à un pavage de* $\mathcal{H}$ *qui utilise des domaines fondamentaux pour l'action de* $\mathrm{SL}_2(\mathbb{Z})$ *(en bas).*

Les matrices $\mathrm{T} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ et $\mathrm{S} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ vérifient $\mathrm{T} \cdot z = z + 1$ et $\mathrm{S} \cdot z = -1/z$. Elles engendrent le groupe $\mathrm{SL}_2(\mathbb{Z})$.

L'*action de poids* k de $\mathrm{SL}_2(\mathbb{Z})$ sur les fonctions $f : \mathcal{H} \to \mathbb{C}$ est définie par

$$(f|_k\gamma)(z) = (cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right)$$

si $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Dans cette notation, les équations fonctionnelles $\mathrm{E}_k(z + 1) =$

$\mathrm{E}_k(z)$ et $\mathrm{E}_k(-1/z) = z^k \mathrm{E}_k(z)$ impliquent que la série d'Eisenstein E_k vérifie $\mathrm{E}_k|_k\gamma = \mathrm{E}_k$ pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ lorsque $k > 2$.

Une *forme modulaire de poids k pour* $\mathrm{SL}_2(\mathbb{Z})$ est une fonction holomorphe $f\colon \mathcal{H} \to \mathbb{C}$ telle que $f|_k\gamma = f$ pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ et telle qu'une condition supplémentaire soit remplie, à savoir être holomorphe à l'infini. Pour énoncer cette condition, notons que prendre $\gamma = \mathrm{T}$ montre que $f(z+1) = f(z)$. Nous pouvons donc développer f en série de Fourier

$$f(z) = \sum_{n\in\mathbb{Z}} a_n\, e^{2\pi i n z}.$$

On dit que f est *méromorphe à l'infini* s'il n'y a qu'un nombre fini de coefficients non nuls a_n avec $n < 0$, et *holomorphe à l'infini* si $a_n = 0$ pour tout $n < 0$. Le nom reflète le fait que cette série de Fourier régit le comportement de $f(z)$ lorsque $\operatorname{Im} z$ tend vers l'infini, car $e^{2\pi i z} \to 0$ lorsque $\operatorname{Im} z \to \infty$. La série de Fourier d'une forme modulaire est souvent appelée « série en q », avec $q = e^{2\pi i z}$.

Le facteur de normalisation $1/(2\zeta(k))$ dans l'équation (1) garantit que la série en q de E_k a des coefficients rationnels, et même des coefficients entiers lorsque k est petit. Par exemple, on peut montrer que

$$\mathrm{E}_4(z) = 1 + 240 \sum_{n\geqslant 1} \sigma_3(n)\, q^n \quad \text{et} \quad \mathrm{E}_6(z) = 1 - 504 \sum_{n\geqslant 1} \sigma_5(n)\, q^n,$$

où $\sigma_k(n)$ désigne la somme des puissances k-ièmes des diviseurs de n.

Le produit de formes modulaires de poids k et ℓ est une forme modulaire de poids $k+\ell$; les formes modulaires forment donc un anneau gradué. Pour $\mathrm{SL}_2(\mathbb{Z})$, on peut montrer que cet anneau est engendré par E_4 et E_6. En d'autres termes, l'espace vectoriel des formes modulaires de poids k pour $\mathrm{SL}_2(\mathrm{Z})$ est engendré par les formes modulaires $\mathrm{E}_4^j \mathrm{E}_6^\ell$ avec $4j + 6\ell = k$.

En plus d'utiliser directement les séries d'Eisenstein, Viazovska utilise également le *discriminant modulaire* Δ, qui est donné par

$$\Delta(z) = \frac{\mathrm{E}_4(z)^3 - \mathrm{E}_6(z)^2}{1728} = q \prod_{n=1}^{\infty} (1 - q^n)^{24}. \tag{2}$$

Sa principale propriété est qu'il ne s'annule pas dans le demi-plan supérieur, alors qu'il s'annule à l'infini (dans le sens où sa série en q n'a pas de terme constant).

Turán a dit que les fonctions spéciales devraient plutôt être appelées fonctions utiles. Les formes modulaires ne font pas exception à ce

principe. La raison pour laquelle nous étudions les formes modulaires n'est pas que nous avons un amour particulier pour les séries d'Eisenstein, mais plutôt que les équations fonctionnelles $f(z+1) = f(z)$ et $f(-1/z) = z^k f(z)$ se présentent bien plus souvent qu'on ne pourrait le croire. Par exemple, au réseau E_8 est associé une forme modulaire importante, à savoir sa *fonction thêta*

$$\Theta_{\mathrm{E}_8}(z) = \sum_{n=0}^{\infty} \mathrm{N}_n \, e^{2\pi i n z},$$

où $\mathrm{N}_n = \#\left\{x \in \mathrm{E}_8 : |x|^2 = 2n\right\}$. En d'autres termes, la fonction thêta est une série génératrice qui compte le nombre de vecteurs de chaque longueur dans E_8.

Cette fonction thêta vérifie deux équations fonctionnelles : $\Theta_{\mathrm{E}_8}(z+1) = \Theta_{\mathrm{E}_8}(z)$ découle de la définition de Θ_{E_8} en tant que série de Fourier, tandis que $\Theta_{\mathrm{E}_8}(-1/z) = z^4 \Theta_{\mathrm{E}_8}$ correspond à la formule sommatoire de Poisson sur E_8 pour la fonction gaussienne complexe $x \mapsto e^{\pi i z |x|^2}$, dont la transformée de Fourier en dimension 8 est $y \mapsto z^{-4} e^{\pi i (-1/z)|y|^2}$. Ces équations fonctionnelles nous indiquent que Θ_{E_8} est une forme modulaire de poids 4 pour $\mathrm{SL}_2(\mathbb{Z})$ et qu'elle doit donc être proportionnelle à E_4. En fait, $\Theta_{\mathrm{E}_8} = \mathrm{E}_4$ car $\mathrm{N}_0 = 1$. On obtient ainsi la belle formule $240\sigma_3(n)$ pour le nombre de vecteurs dans E_8 dont le carré de la norme vaut $2n$.

La théorie des formes modulaires s'étend à d'autres groupes discrets, si l'on définit soigneusement ce que signifie être holomorphe à l'infini [3]. La démonstration de Viazovska fait appel à un groupe supplémentaire, à savoir

$$\Gamma(2) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2 \right\},$$

qui est d'indice 6 dans $\mathrm{SL}_2(\mathbb{Z})$. Si l'on pose

$$\mathrm{U}(z) = \left(\sum_{n \in \mathbb{Z}} e^{\pi i n^2 z} \right)^4,$$

3. Si Γ est un sous-groupe d'indice fini dans $\mathrm{SL}_2(\mathbb{Z})$, alors la condition est que pour tout $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $f|_k\gamma$ doit être holomorphe à l'infini. Notons que $f|_k\gamma$ ne doit pas nécessairement vérifier $(f|_k\gamma)(z+1) = (f|_k\gamma)(z)$, mais on peut remarquer qu'il vérifie toujours $(f|_k\gamma)(z+n) = (f|_k\gamma)(z)$ pour un entier strictement positif n et qu'il a donc un développement de Fourier en $e^{2\pi i z/n} = q^{1/n}$.

$W = U|_2 T$ et $V = U - W$, alors U, V et W sont des formes modulaires de poids 2 pour $\Gamma(2)$ qui vérifient $U = V + W$ et

$$\begin{aligned} U|_2 T &= W, \quad V|_2 T = -V, \quad W|_2 T = U, \\ U|_2 S &= -U, \quad V|_2 S = -W, \quad W|_2 S = -V. \end{aligned} \tag{3}$$

Ces identités joueront un rôle clé dans la construction de la fonction magique de Viazovska. Il s'avère que U et W engendrent l'anneau des formes modulaires pour $\Gamma(2)$. Donc toute forme modulaire de poids $2k$ pour $\Gamma(2)$ est une combinaison linéaire de U^k, $U^{k-1}W$, $U^{k-2}W^2$, …, W^k.

Les formes modulaires étant étroitement liées aux réseaux, il est naturel de se tourner vers les formes modulaires pour tenter de construire les fonctions magiques. Cependant, il n'est pas du tout évident de savoir par où commencer, car les formes modulaires sont des objets complètement différents des fonctions radiales de Schwartz. La figure 6 ne ressemble en rien aux figures 4 ou 5, et aucune transformation familière ne les rend plus semblables.

4 La construction de Viazovska pour les racines simples

La première étape de la construction par Viazovska de la fonction magique f consiste à décomposer f en fonctions propres de la transformée de Fourier. Les fonctions radiales vérifient

$$\widehat{\widehat{f}} = f.$$

Nous pouvons donc écrire f sous la forme $f = f_+ + f_-$, où

$$f_+ := \frac{f + \widehat{f}}{2} \quad \text{et} \quad f_- := \frac{f - \widehat{f}}{2}$$

vérifient $\widehat{f_+} = f_+$ et $\widehat{f_-} = -f_-$. Si f est la fonction magique en dimension 8, alors f et $\widehat{f}$ ont tous deux des racines en $\sqrt{2n}$ pour tout entier $n \geqslant 1$, donc f_+ et f_- aussi. Nous recherchons donc des fonctions propres de Fourier radiales dont les racines sont spécifiées. Plus précisément, chacune des fonctions $f_\pm$ devrait avoir une racine simple en $\sqrt{2}$ et des racines doubles en $\sqrt{2n}$ pour $n \geqslant 2$. Ces racines fournissent suffisamment d'information pour déterminer $f_\pm$ à l'échelle près. Elles peuvent ensuite être combinées pour obtenir f.

Avant de construire la fonction magique proprement dite, il convient d'examiner une variante plus simple à titre d'exercice d'échauffement.

Au lieu d'essayer de contrôler le comportement de f au second ordre en $\sqrt{2n}$, nous allons plutôt contrôler le comportement d'une fonction g au premier ordre en $\sqrt{n}$. Cette construction n'a pas d'application connue dans le domaine de l'empilement de sphères, mais elle est néanmoins d'un intérêt intrinsèque en analyse harmonique. Nous nous concentrerons également sur la valeur propre -1 (c'est-à-dire le cas $\widehat{g} = -g$) dans le cas de la racine simple, pour fixer les idées.

Viazovska a trouvé une transformée intégrale remarquable qui permet de construire de telles fonctions. Nous écrirons une fonction radiale $g\colon \mathbb{R}^8 \to \mathbb{C}$ comme une combinaison linéaire continue de gaussiennes complexes $x \mapsto e^{\pi i z|x|^2}$ avec $z \in \mathcal{H}$ *via* l'intégrale de contour

$$g(x) = \tfrac{1}{2} \int_{-1}^{1} \psi(z)\, e^{\pi i z|x|^2}\, dz, \tag{4}$$

où ψ est une fonction holomorphe sur $\mathcal{H}$ et le contour est un demi-cercle dont le centre est l'origine. À quelles conditions sur ψ la fonction g sera-t-elle une fonction propre de Fourier et comment pouvons-nous contrôler ses valeurs en $\sqrt{n}$?

Nous pouvons obtenir les valeurs $g\left(\sqrt{n}\right)$ en imposant à ψ d'être périodique comme suit. Supposons que $\psi(z+2) = \psi(z)$ pour tout $z \in \mathcal{H}$, de sorte que ψ a une série de Fourier de la forme

$$\psi(z) = \sum_{n \in \mathbb{Z}} a_n\, e^{\pi i n z}. \tag{5}$$

Alors pour tout entier $n \geqslant 0$,

$$g\left(\sqrt{n}\right) = \tfrac{1}{2} \int_{-1}^{1} \psi(z)\, e^{\pi i n z}\, dz = a_{-n}$$

par orthogonalité, à condition que l'on puisse intervertir la somme et l'intégrale. Si le développement en série de Fourier (5) n'a qu'un nombre fini de termes négatifs, alors $g\left(\sqrt{n}\right)$ s'annulera pour tous les n sauf pour un nombre fini d'entre eux.

Pour calculer la transformée de Fourier de g, nous pouvons intervertir l'intégrale de contour et la transformée de Fourier, en supposant à nouveau que l'intégrale se comporte suffisamment bien. Alors

$$\widehat{g}(y) = \tfrac{1}{2} \int_{-1}^{1} \psi(z)\, z^{-4}\, e^{\pi i(-1/z)|y|^2}\, dz,$$

car la transformée de Fourier en dimension d de la gaussienne complexe $x \mapsto e^{\pi i z|x|^2}$ avec $z \in \mathcal{H}$ est donnée par $y \mapsto (i/z)^{d/2} e^{\pi i(-1/z)|y|^2}$, et $d = 8$ ici. Le changement de variable $u = -1/z$ montre que

$$\widehat{g}(y) = -\tfrac{1}{2} \int_{-1}^{1} \psi(-1/u)\, u^2\, e^{\pi i u|y|^2}\, du.$$

En d'autres termes, prendre la transformée de Fourier de g revient à remplacer ψ par $-\psi|_{-2}\mathrm{S}$. Nous obtenons $\widehat{g} = -g$ si $\psi|_{-2}\mathrm{S} = \psi$.

Soit Γ le sous-groupe de $\mathrm{SL}_2(\mathbb{Z})$ engendré par S et T^2, qui a un indice 3 dans $\mathrm{SL}_2(\mathbb{Z})$. Les conditions $\psi|_{-2}\mathrm{T}^2 = \psi$, c'est-à-dire $\psi(z+2) = \psi(z)$, et $\psi|_{-2}\mathrm{S} = \psi$ signifient que ψ est *faiblement modulaire de poids* -2 pour Γ. La raison pour laquelle ψ n'est pas une forme modulaire à part entière est qu'elle n'est que méromorphe à l'infini, ce qui est inévitable puisque le poids est négatif. Nous avons en outre besoin que ψ s'annule en ± 1, ce qui suffira à justifier nos manipulations d'intégrales et à montrer que g est une fonction de Schwartz. En termes de séries de Fourier, cette annulation signifie que $\psi|_{-2}\mathrm{TS}$ n'a pas de termes négatifs dans sa série en q, car TS envoie la pointe $i\infty$ sur 1.

Nous allons construire un exemple de la forme $\psi = \psi_0/\Delta$ en utilisant la fonction Δ de l'équation (2), où ψ_0 est une véritable forme modulaire de poids 10 pour Γ. Notons que le dénominateur de Δ ne pose aucune difficulté dans $\mathcal{H}$, puisque $\Delta(z) \neq 0$ pour tout $z \in \mathcal{H}$, et que le zéro de Δ à l'infini conduira à un pôle pour ψ.

La fonction ψ_0 est modulaire de poids 10 pour Γ et donc aussi pour $\Gamma(2)$, car $\Gamma(2)$ est un sous-groupe de Γ. En particulier, ψ_0 doit être une combinaison linéaire de U^5, $\mathrm{U}^4\mathrm{W}$, $\mathrm{U}^3\mathrm{W}^2$, …, W^5, parce que U et W engendrent l'anneau des formes modulaires pour $\Gamma(2)$. Les relations (3) spécifient l'action de S et T ; elles impliquent que le sous-espace stable par S est engendré par

$$\begin{aligned}
\alpha &:= \mathrm{U}^5 - 6\,\mathrm{U}^3\mathrm{W}^2 + 4\,\mathrm{U}^2\mathrm{W}^3, \\
\beta &:= \mathrm{U}^4\mathrm{W} - 3\,\mathrm{U}^3\mathrm{W}^2 + 2\,\mathrm{U}^2\mathrm{W}^3 \text{ et} \\
\gamma &:= -\mathrm{U}^3\mathrm{W}^2 + 4\,\mathrm{U}^2\mathrm{W}^3 - 5\,\mathrm{U}\mathrm{W}^4 + 2\,\mathrm{W}^5,
\end{aligned}$$

avec des séries en q

$$\frac{\alpha}{\Delta} = -q^{-1} - 40\,q^{-1/2} + 752 + \cdots, \quad \frac{\alpha}{\Delta}\Big|_{-2}\mathrm{TS} = -1024 + 90112\,q + \cdots,$$
$$\frac{\beta}{\Delta} = -16\,q^{-1/2} + 256 + \cdots, \quad \frac{\beta}{\Delta}\Big|_{-2}\mathrm{TS} = -512 - 20480\,q + \cdots,$$
$$\frac{\gamma}{\Delta} = 256 - 10240\,q^{1/2} + \cdots, \quad \frac{\gamma}{\Delta}\Big|_{-2}\mathrm{TS} = -2\,q^{-1} - 32 + \cdots$$

avec $q^{1/2} = e^{\pi i z}$. Le fait d'exiger que la fonction ψ s'annule en ± 1 la détermine à l'échelle près sous la forme

$$\psi = \frac{2\beta - \alpha}{\Delta} = q^{-1} + 8\,q^{-1/2} - 240 - 6176\,q^{1/2} - \cdots, \tag{6}$$

ce qui donne une fonction de Schwartz radiale $g\colon \mathbb{R}^8 \to \mathbb{R}$ telle que $\widehat{g} = -g$ et

$$g\left(\sqrt{n}\right) = \begin{cases} -240 & \text{si } n = 0, \\ 8 & \text{si } n = 1, \\ 1 & \text{si } n = 2, \\ 0 & \text{si } n \geqslant 3. \end{cases}$$

Nous pouvons réécrire la définition de f sous une autre forme utile. Si $|x|$ est suffisamment grand (en fait $|x|^2 > 2$ suffit), alors

$$\begin{aligned} g(x) &= \tfrac{1}{2}\int_{-1}^{1} \psi(z)\, e^{\pi i z|x|^2}\, dz \\ &= \tfrac{1}{2}\int_{-1}^{i} \psi(z)\, e^{\pi i z|x|^2}\, dz - \tfrac{1}{2}\int_{1}^{i} \psi(z)\, e^{\pi i z|x|^2}\, dz \\ &= \tfrac{1}{2}\int_{-1}^{-1+i\infty} \psi(z)\, e^{\pi i z|x|^2}\, dz - \tfrac{1}{2}\int_{1}^{1+i\infty} \psi(z)\, e^{\pi i z|x|^2}\, dz \\ &= \frac{e^{-\pi i|x|^2} - e^{\pi i|x|^2}}{2}\int_{0}^{i\infty} \psi(u+1)\, e^{\pi i u|x|^2}\, du. \end{aligned}$$

Dans ces manipulations, la deuxième ligne se contente de scinder l'intégrale en deux, la troisième ligne utilise le fait que

$$\int_{-1+i\mathrm{R}}^{1+i\mathrm{R}} \psi(z)\, e^{\pi i z|x|^2}\, dz \to 0$$

quand $\mathrm{R} \to \infty$ (ce qui est le cas si $|x|^2$ est suffisamment grand), et la quatrième ligne utilise $\psi(u-1) = \psi(u+1)$.

En d'autres termes, $g(x)$ est donné par $\sin(\pi|x|^2)$ multiplié par la transformée de Laplace de $t \mapsto \psi(it+1)$ évaluée en $\pi|x|^2$:

$$g(x) = \sin(\pi|x|^2) \int_0^\infty \psi(it+1) e^{-\pi t|x|^2}\, dt. \tag{7}$$

Alors que l'intégrale originale (4) converge pour tous les x, cette intégrale ne converge que lorsque $|x|^2$ est suffisamment grand pour que le facteur gaussien $e^{-\pi t|x|^2}$ contrebalance la croissance de $\psi(it+1)$ lorsque $t \to \infty$. En particulier, l'équation (6) implique que

$$\psi(it+1) = e^{2\pi t} - 8\, e^{\pi t} - 240 + 6176\, e^{-\pi t} - \cdots$$

lorsque $t \to \infty$, ce qui signifie que nous avons besoin de $|x|^2 > 2$. Nous pouvons utiliser ce développement pour prolonger analytiquement g en enlevant les termes qui divergent :

$$\begin{aligned} g(x) &= \sin(\pi|x|^2) \int_0^\infty \Big(e^{2\pi t} - 8\, e^{\pi t} - 240\Big) e^{-\pi t|x|^2}\, dt \\ &\quad + \sin(\pi|x|^2) \int_0^\infty \Big(\psi(it+1) - e^{2\pi t} + 8\, e^{\pi t} + 240\Big) e^{-\pi t|x|^2}\, dt \\ &= \frac{\sin(\pi|x|^2)}{\pi(|x|^2-2)} - \frac{8\sin(\pi|x|^2)}{\pi(|x|^2-1)} - \frac{240\sin(\pi|x|^2)}{\pi|x|^2} \\ &\quad + \sin(\pi|x|^2) \int_0^\infty \Big(\psi(it+1) - e^{2\pi t} + 8\, e^{\pi t} + 240\Big) e^{-\pi t|x|^2}\, dt, \end{aligned}$$

et cette dernière formule est valable quel que soit $|x|$, avec des singularités effaçables en $|x| = 0$, 1 et $\sqrt{2}$.

5 La construction de Viazovska pour les racines doubles

Nous sommes maintenant en mesure d'obtenir la fonction magique en dimension 8. Nous obtiendrons tout d'abord la fonction propre f_- associée à la valeur propre -1 . Il n'est pas évident de généraliser l'intégrale de contour (4) des racines simples aux racines doubles, mais la formule de la transformée de Laplace (7) se généralise élégamment. Pour obtenir f_-, nous chercherons une fonction spéciale ψ telle que

$$f_-(x) = -4\, i \sin\left(\pi|x|^2/2\right)^2 \int_0^{i\infty} \psi(z)\, e^{\pi i z|x|^2}\, dz$$

lorsque $|x|$ est suffisamment grand. En écrivant $-4\sin(\pi|x|^2/2)^2 = e^{-\pi i|x|^2} + e^{\pi i|x|^2} - 2$, on trouve que

$$f_-(x) = \int_{-1}^{-1+i\infty} \psi(z+1)\, e^{\pi i|x|^2 z}\, dz + \int_{1}^{1+i\infty} \psi(z-1)\, e^{\pi i|x|^2 z}\, dz - 2\int_{0}^{i\infty} \psi(z)\, e^{\pi i|x|^2 z}\, dz.$$

Nous allons construire une fonction ψ telle que ψ soit holomorphe sur $\mathcal{H}$ et $\psi(z)$ soit exponentiellement bornée lorsque $\operatorname{Im} z \to \infty$. Sous ces conditions, lorsque $|x|$ est suffisamment grand, on peut déplacer les contours et combiner les intégrales pour obtenir

$$f_-(x) = \int_{-1}^{i} \psi(z+1)\, e^{\pi i|x|^2 z}\, dz + \int_{1}^{i} \psi(z-1)\, e^{\pi i|x|^2 z}\, dz - 2\int_{0}^{i} \psi(z)\, e^{\pi i|x|^2 z}\, dz + \int_{i}^{i\infty} \left(\psi(z+1) + \psi(z-1) - 2\psi(z)\right) e^{\pi i|x|^2 z}\, dz,$$

avec les contours indiqués dans la figure 7. Cette formule sera l'analogue de l'équation (4) et elle définira $f_-(x)$ pour tout x.

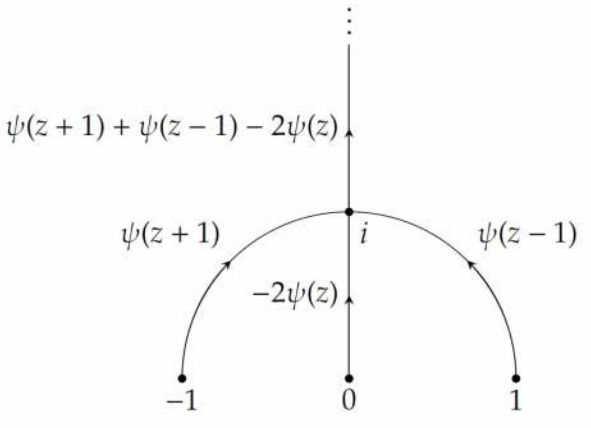


FIG. 7 – *Les contours utilisés pour obtenir $f_-(x)$, étiquetés avec leurs intégrandes (en omettant $e^{\pi i|x|^2 z}\, dz$).*

Prendre la transformée de Fourier revient à remplacer $e^{\pi i|x|^2 z}$ par

$z^{-4}e^{\pi i|y|^2(-1/z)}$ dans la formule qui définit f_- :

$$\begin{aligned}\widehat{f_-}(y) = &\int_{-1}^{i} \psi(z+1)\, z^{-4}\, e^{\pi i|y|^2(-1/z)}\, dz + \int_{1}^{i} \psi(z-1)\, z^{-4}\, e^{\pi i|y|^2(-1/z)}\, dz \\ &- 2\int_{0}^{i} \psi(z)\, z^{-4}\, e^{\pi i|y|^2(-1/z)}\, dz \\ &+ \int_{i}^{i\infty} (\psi(z+1) + \psi(z-1) - 2\psi(z))\, z^{-4}\, e^{\pi i|y|^2(-1/z)}\, dz.\end{aligned}$$

On peut maintenant poser $u = -1/z$, ce qui échange les quatre contours deux à deux. La façon la plus simple d'obtenir $\widehat{f_-} = -f_-$ serait que la formule résultante soit exactement l'opposée de la formule par laquelle nous avons commencé. Cela se traduit par les équations fonctionnelles

$$\psi|_{-2}\mathrm{TS} = -\psi|_{-2}\mathrm{T}^{-1}$$

et

$$2\,\psi|_{-2}\mathrm{S} = 2\,\psi - \psi|_{-2}\mathrm{T} - \psi|_{-2}\mathrm{T}^{-1}.$$

Notons que la structure de ces équations reflète les différents intégrandes.

La question est maintenant de savoir quelles sortes de fonctions ψ vérifient ces équations fonctionnelles. La possibilité la plus simple serait une sorte de forme modulaire. Les équations fonctionnelles ne sont pas compatibles avec l'invariance par S et T, donc ψ ne peut pas être modulaire pour le groupe complet $\mathrm{SL}_2(\mathbb{Z})$. Supposons plutôt que ψ soit faiblement modulaire de poids -2 pour $\Gamma(2)$ (c'est-à-dire invariant par $\Gamma(2)$ mais seulement méromorphe à l'infini). Alors $\psi|_{-2}\mathrm{T} = \psi|_{-2}\mathrm{T}^{-1}$, car $\mathrm{T}^2 \in \Gamma(2)$, et nos équations fonctionnelles deviennent $\psi|_{-2}\mathrm{TS} = -\psi|_{-2}\mathrm{T}$ et $\psi = \psi|_{-2}\mathrm{T} + \psi|_{-2}\mathrm{S}$. De plus, la deuxième équation implique la première, car $\mathrm{S}^2 = \mathrm{I}$. On obtient donc l'équation pour la fonction propre $\widehat{f_-} = -f_-$ si ψ est faiblement modulaire de poids -2 pour $\Gamma(2)$ et vérifie $\psi = \psi|_{-2}\mathrm{T} + \psi|_{-2}\mathrm{S}$.

Comme dans le cas des racines simples, il est naturel de multiplier ψ par Δ pour essayer d'éliminer un pôle à l'infini. Alors $\psi\Delta$ sera une véritable forme modulaire de poids 10 pour $\Gamma(2)$, et donc une combinaison linéaire de U^5, $\mathrm{U}^4\mathrm{W}$, $\mathrm{U}^3\mathrm{W}^2$, . . ., W^5. On peut vérifier que les solutions de l'équation fonctionnelle restante forment un sous-espace bidimensionnel engendré par

$$\alpha := 2\,\mathrm{U}^4\mathrm{W} - 4\,\mathrm{U}^3\mathrm{W}^2 + \mathrm{U}^2\mathrm{W}^3 + \mathrm{U}\mathrm{W}^4$$

et

$$\beta := 5\,\mathrm{U}^4\mathrm{W} - 10\,\mathrm{U}^3\mathrm{W}^2 + 5\,\mathrm{U}^2\mathrm{W}^3 + \mathrm{W}^5,$$

avec

$$\frac{\alpha}{\Delta} = -16\,q^{-1/2} + 768 + \cdots$$

et

$$\frac{\beta}{\Delta} = q^{-1} - 40\,q^{-1/2} + 2064 + \cdots$$

Nous prendrons

$$\psi = \frac{-5\,\alpha + 2\,\beta}{\Delta} = 2\,q^{-1} + 288 + \cdots,$$

de façon à éliminer le terme $q^{-1/2}$ dans la série en q. La motivation pour éliminer ce terme est qu'il empêche f_- d'avoir un pôle au rayon 1. Pour comprendre pourquoi, prolongeons analytiquement

$$f_-(x) = 4\sin(\pi|x|^2/2)^2 \int_0^\infty \psi(it)\, e^{-\pi t|x|^2}\, dt$$

comme dans le cas de la racine simple. Si $\psi(it) = a_2 e^{2\pi t} + a_1 e^{\pi t} + a_0 + \cdots$ quand $t \to \infty$, alors

$$\begin{aligned} f_-(x) = {} & \frac{4\,a_2 \sin(\pi|x|^2/2)^2}{\pi(|x|^2 - 2)} - \frac{4\,a_1 \sin(\pi|x|^2/2)^2}{\pi(|x|^2 - 1)} - \frac{4\,a_0 \sin(\pi|x|^2/2)^2}{\pi|x|^2} \\ & + 4\sin(\pi|x|^2/2)^2 \int_0^\infty \left(\psi(it) - a_2 e^{2\pi t} - a_1 e^{\pi t} - a_0\right) e^{-\pi t|x|^2}\, dt. \end{aligned}$$

Le terme a_1 a ici un pôle à moins que $a_1 = 0$. Pour notre choix de ψ, $(a_2, a_1, a_0) = (2, 0, 288)$, donc f_- a une racine simple en $\sqrt{2}$ et des racines doubles en $\sqrt{2n}$ pour tout $n \geqslant 2$. On peut aussi vérifier que $\psi(it)$ tend vers 0 lorsque $t \to 0^+$ (de façon équivalente, $\psi|_{-2}\mathrm{S}$ tend vers 0 à l'infini), ce qui est suffisant pour que f_- soit une fonction de Schwartz et pour justifier toutes nos manipulations avec les intégrales.

Nous avons donc obtenu une fonction propre magique f_- sous la forme

$$f_-(x) = 4\sin(\pi|x|^2/2)^2 \int_0^\infty \psi(it)\, e^{-\pi t|x|^2}\, dt$$

pour $|x|^2 > 2$, où

$$\psi = \frac{\mathrm{W}^3(5\,\mathrm{U}^2 - 5\,\mathrm{UW} + 2\,\mathrm{W}^2)}{\Delta}. \tag{8}$$

Notre mise à l'échelle ne correspond pas encore à la fonction magique pour l'empilement de sphères. Mais à part cela, nous avons exactement ce dont nous avons besoin.

L'équation (8) implique que $\psi(it) > 0$ pour tout $t \in]0,\infty[$ [§]. Il s'ensuit que f_- ne change jamais de signe au-delà du rayon $\sqrt{2}$, conformément à nos attentes. Notons cependant que notre fonction propre est strictement positive au-delà du rayon $\sqrt{2}$; nous devrons donc corriger son signe ultérieurement pour qu'il corresponde à celui de la fonction magique.

Il ne reste plus qu'à construire une fonction propre magique f_+ et à prendre une combinaison linéaire appropriée de f_+ et f_- pour obtenir f. La construction de f_+ est très similaire à la construction de f_-. Si nous définissons f_+ pour $|x|$ suffisamment grand par

$$f_+(x) = -4i \sin(\pi|x|^2/2)^2 \int_0^{i\infty} \varphi(z)\, e^{\pi i z|x|^2}\, dz$$

avec une fonction holomorphe $\varphi\colon \mathcal{H} \to \mathbb{C}$, alors l'équation de la fonction propre $\widehat{f_+} = f_+$ découlera des équations fonctionnelles

$$\varphi|_{-2}\mathrm{TS} = \varphi|_{-2}\mathrm{T}^{-1}$$

et

$$2\,\varphi|_{-2}\mathrm{S} = -2\,\varphi + \varphi|_{-2}\mathrm{T} + \varphi|_{-2}\mathrm{T}^{-1}.$$

Il s'agit des mêmes équations fonctionnelles que celles requises pour ψ, à part un facteur -1.

Une petite manipulation à l'aide de $(\mathrm{ST})^3 = \mathrm{I}$ montre que la première équation fonctionnelle est équivalente à $\varphi|_{-2}\mathrm{ST} = \varphi|_{-2}\mathrm{S}$. Ainsi, si nous posons $\chi := \varphi|_{-2}\mathrm{S}$, alors χ doit être invariant par T. Cependant, la seconde équation fonctionnelle est plus subtile. Un bref calcul montre que si $\chi|_0\mathrm{S} = \chi$ (ou de manière équivalente $(\chi|_{-2}\mathrm{S})(z) = z^2\chi(z)$), alors la deuxième équation fonctionnelle est vérifiée. Il suffit en d'autres termes que χ soit faiblement modulaire de poids 0 pour $\mathrm{SL}_2(\mathbb{Z})$. Mais de telles fonctions ne sont pas suffisantes pour obtenir f_+. Si l'on cherche des coefficients indéterminés pour construire f_+ comme dans le cas de f_-, on trouve qu'il n'y a pas de solution avec les propriétés requises.

Au lieu de cela, nous pouvons utiliser des *formes quasi-modulaires*, pas seulement des formes modulaires. Rappelons que la série d'Eisenstein

§. Plus précisément, $\Delta(it) > 0$ grâce à sa formule comme produit, $\mathrm{W}(it) > 0$ puisqu'il s'agit de la puissance quatrième d'une quantité réelle, et $5\,\mathrm{U}(it)^2 - 5\,\mathrm{U}(it)\mathrm{W}(it) + 2\,\mathrm{W}(it)^2 > 0$ puisqu'il s'agit d'une forme quadratique définie positive.

E_2 n'était pas une forme modulaire de poids 2, car la semi-convergence interférait avec les manipulations de séries nécessaires pour démontrer la modularité. Si nous posons

$$\mathrm{E}_2(z) = 1 - 24 \sum_{n \geqslant 1} \sigma_1(n)\, q^n,$$

alors E_2 vérifie

$$z^{-2}\mathrm{E}_2(-1/z) = \mathrm{E}_2(z) - \frac{6\,i}{\pi z}.$$

Le terme $6\,i/(\pi z)$ correspondant à l'écart par rapport à la modularité. Une *forme quasi-modulaire de poids k et de profondeur ℓ* pour $\mathrm{SL}_2(\mathbb{Z})$ est une somme $f_k + f_{k-2}\mathrm{E}_2 + \cdots + f_{k-\ell}\mathrm{E}_2^\ell$, où chaque f_j est une forme modulaire de poids $k - 2j$.

Au lieu d'une simple forme faiblement modulaire de poids 0, on peut vérifier que la fonction χ peut être une forme faiblement quasi-modulaire de poids 0 et de profondeur 2 pour $\mathrm{SL}_2(\mathbb{Z})$. Nous avons maintenant assez de flexibilité pour construire f_+. Des calculs similaires à ceux effectués dans le cas de f_- conduisent à

$$\chi = \frac{(\mathrm{E}_2\mathrm{E}_4 - \mathrm{E}_6)^2}{\Delta},$$

à l'échelle près. Voir la figure 8 pour les tracés des formes quasi-modulaires qui donnent f_- et f_+.

Maintenant que nous avons obtenu les deux fonctions propres magiques, nous pouvons construire la fonction magique f comme une combinaison linéaire de celles-ci. Nous changeons tout d'abord l'échelle de φ pour que $f_+(0) = 1$, puis nous changeons l'échelle de ψ pour que $f_-'\left(\sqrt{2}\right) = f_+'\left(\sqrt{2}\right)$, afin d'obtenir une racine double en $\sqrt{2}$ pour $\widehat{f}$. En utilisant ces échelles, la fonction magique en dimension 8 est donnée par

$$f(x) = 4\sin(\pi|x|^2/2)^2 \int_0^\infty \left(\varphi(it) + \psi(it)\right)\, e^{-\pi t|x|^2}\, dt$$

pour $|x|^2 > 2$. La propriété de fonction propre implique que

$$\widehat{f(y)} = 4\sin(\pi|y|^2/2)^2 \int_0^\infty \left(\varphi(it) - \psi(it)\right) e^{-\pi t|y|^2}\, dt$$

pour tout $y \neq 0$. Il s'avère que cette intégrale converge dès que $|y| > 0$, car les croissances exponentielles de $\varphi(it)$ et $\psi(it)$ quand $t \to \infty$ se compensent.

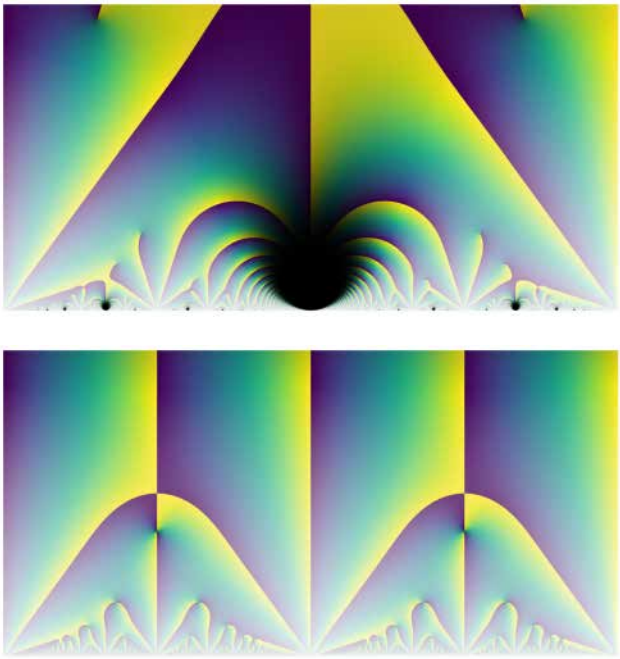


FIG. 8 – *Tracés de* $\psi(z)\Delta(z)$ *(en haut) et* $\varphi|_{-2}\mathrm{S})(z)\Delta(z)$ *(en bas) pour* $-1 \leqslant \operatorname{Re} z \leqslant 1$ *et* $0 < \operatorname{Im} z \leqslant 1$.

La dernière étape de la démonstration du théorème 5 consiste à vérifier les inégalités nécessaires au théorème 7, à savoir $f(x) \leqslant 0$ pour $|x| \geqslant 2$ et $\widehat{f(y)} \geqslant 0$ pour tout y, afin de s'assurer qu'il n'y a pas de changement de signe inattendu entre les racines $\sqrt{2n}$. En principe, cela peut sembler difficile, car les transformations intégrales des formes quasi-modulaires pourraient être compliquées. Mais ces inégalités sont valables pour la raison la plus simple que l'on puisse espérer :

$$\varphi(it) + \psi(it) < 0 \quad \text{et} \quad \varphi(it) - \psi(it) > 0$$

pour tout $t > 0$. En d'autres termes, les inégalités souhaitées s'appliquent directement au niveau des formes quasi-modulaires elles-mêmes. On peut vérifier ceci rigoureusement de plusieurs façons. Par exemple, on peut utiliser le comportement asymptotique pour vérifier les inégalités

lorsque $t \to 0$ ou $t \to \infty$, puis utiliser l'arithmétique d'intervalles pour les vérifier sur l'intervalle borné restant.

Dans l'ensemble, cette démonstration tient du miracle. Tout se met merveilleusement en place, les constructions de Viazovska ayant juste assez de flexibilité pour compléter la démonstration d'une manière unique. Ce que je trouve le plus impressionnant, c'est le nombre d'idées ingénieuses requises pour la démonstration complète. La construction pour la racine simple est en elle-même remarquable, la généraliser à f_- l'est encore plus, et encore plus d'idées sont nécessaires pour f_+. Viazovska est passée maître en fonctions spéciales. Ses travaux auraient certainement enthousiasmé Jacobi et Ramanujan.

6 Interpolation et conséquences

Tout en démontrant l'optimalité de E_8, Viazovska a fait la conjecture audacieuse que la fonction magique est déterminée de façon unique par les racines requises et que, plus généralement, une fonction de Schwartz radiale sur $\mathbb{R}^8$ est déterminée de façon unique par ses valeurs et ses dérivées radiales aux rayons $\sqrt{2n}$ ainsi que par celles de sa transformée de Fourier. Il est loin d'être évident qu'il soit possible en principe de reconstruire une fonction de Schwartz radiale à partir de données discrètes de ce type.

Radchenko et Viazovska ont fait un grand pas dans cette direction en démontrant un analogue unidimensionnel pour l'interpolation du premier ordre. Le théorème du second ordre a été démontré par Cohn, Kumar, Miller, Radchenko et Viazovska.

Théorème 8 (Radchenko et Viazovska [23])**.** *Il existe des fonctions de Schwartz $a_n \colon \mathbb{R} \to \mathbb{R}$ telles que pour toute fonction de Schwartz $f \colon \mathbb{R} \to \mathbb{R}$ et tout $x \in \mathbb{R}$,*

$$f(x) = \sum_{n \in \mathbb{Z}} f\left(\sqrt{n}\right) a_n(x) + \sum_{n \in \mathbb{Z}} \widehat{f}\left(\sqrt{n}\right) \widehat{a_n}(x).$$

Théorème 9 (Cohn, Kumar, Miller, Radchenko et Viazovska [11])**.** *Soit (d, n_0) égal à $(8, 1)$ ou $(24, 2)$. Alors toute fonction de Schwartz radiale $f \colon \mathbb{R}^d \to \mathbb{R}$ est déterminée de façon unique par les valeurs $f\left(\sqrt{2n}\right)$, $f'\left(\sqrt{2n}\right)$, $\widehat{f}\left(\sqrt{2n}\right)$ et $\widehat{f}'\left(\sqrt{2n}\right)$ pour tout entier $n \geqslant n_0$. Plus précisément, il existe une base d'interpolation a_n, b_n pour $n \geqslant n_0$ telle que pour toute fonction de*

Schwartz radiale f et tout $x \in \mathbb{R}^d$,

$$f(x) = \sum_{n=n_0}^{\infty} f\left(\sqrt{2n}\right) a_n(x) + \sum_{n=n_0}^{\infty} f'\left(\sqrt{2n}\right) b_n(x) + \sum_{n=n_0}^{\infty} \widehat{f}\left(\sqrt{2n}\right) \widehat{a_n}(x) + \sum_{n=n_0}^{\infty} \widehat{f'}\left(\sqrt{2n}\right) \widehat{b_n}(x).$$

Les démonstrations construisent les bases d'interpolation explicitement, en combinant les techniques de transformée intégrale de Viazovska avec des classes plus larges de fonctions spéciales.

Une conséquence de l'interpolation de Fourier radiale est un théorème d'optimalité plus fort pour E_8 et pour le réseau de Leech. Au lieu de prendre en compte uniquement les interactions locales entre les particules comme dans le problème de l'empilement de sphères, on peut étudier les problèmes d'optimisation avec des interactions à longue portée. On peut par exemple chercher à connaître l'état fondamental de particules qui interagissent par l'intermédiaire d'une loi de puissance inverse. Cohn et Kumar [9] ont introduit une notion plus large d'optimalité, appelée « optimalité universelle », et l'interpolation de Fourier radiale produit des fonctions magiques correspondantes :

Théorème 10 (Cohn, Kumar, Miller, Radchenko et Viazovska [11])**.** *Le réseau* E_8 *et le réseau de Leech sont universellement optimaux respectivement dans* $\mathbb{R}^8$ *et* $\mathbb{R}^{24}$*.*

7 L'avenir

Bien que les travaux de Viazovska aient permis de résoudre plusieurs questions majeures, il reste encore beaucoup de choses à comprendre. Par exemple, la théorie de l'interpolation pour les fonctions de Schwartz radiales se développe rapidement, avec des liens notables avec la théorie de l'unicité pour l'équation de Klein-Gordon [2].

L'un des problèmes les plus complexes est celui de la dimension 2. Si le problème de l'empilement de sphères en dimension 2 peut être résolu par la géométrie élémentaire, l'optimalité universelle reste une conjecture séduisante. Il semble y avoir une fonction magique pour $d = 2$ dans le théorème 7, avec $r = (4/3)^{1/4}$. On ne connaît aucune démonstration, mais les calculs numériques concordent avec la densité d'empilement optimale dans $\mathbb{R}^2$ jusqu'à plus de mille chiffres après la virgule. Des fonctions magiques analogues semblent en outre exister

pour l'optimalité universelle dans $\mathbb{R}^2$. On ne sait pas cependant quel type d'espace fonctionnel pourrait permettre une théorie d'interpolation appropriée (voir la section 7 dans [11]).

Il existe également des liens remarquables avec la théorie conforme des champs et la gravité quantique [18]. Lorsque d est pair, la borne de programmation linéaire pour la densité d'empilement de sphères dans $\mathbb{R}^d$ s'avère être équivalente à la borne *bootstrap* modulaire sans spin pour le trou spectral dans une théorie à $d/2$ bosons libres. Le programme du *bootstrap* conforme la généralise à une famille de bornes apparentées. La manière dont ces bornes plus générales peuvent être liées à la géométrie discrète reste un mystère.

Bibliographie

[1] *J. High Energy Phys.*, 2020, article 66

[2] *Proc. Natl. Acad. Sci. USA*, n° 118, 2021, article 2023227118.

[3] *Ann. Math.*, n° 178, 2013, p. 443-452.

[4] *Ann. Inst. Fourier*, n° 60, 2010, p. 1215-1232.

[5] Cohen (Henri) et Strömberg (Fredrik), *Modular Forms : A Classical Approach*, American Mathematical Society, 2017.

[6] *Not. Am. Math. Soc.*, n° 64, 2017, p. 102-115.

[7] *Ann. Math.*, n° 157, 2003, p. 689-714.

[8] *Invent. Math.*, n° 217, 2019, p. 799-831.

[9] *J. Am. Math. Soc.*, n° 20, 2007, p. 99-148.

[10] *Ann. Math.*, n° 185, 2017, p. 1017-1033.

[11] *Ann. Math.*, n° 196, 2022, p. 983-1082.

[12] Conway (John H.) et Sloane (Neil J. A.), *Sphere Packings, Lattices and Groups*, 3e éd., Springer, 1999.

[13] *Philips Res. Rep.*, n° 27, 1972, p. 272-289.

[14] Diamond (Fred) et Shurman (Jerry), *A First Course in Modular Forms*, Springer, 2005.

[15] Ebeling (Wolfgang), *Lattices and Codes*, 3e éd., Springer, 2013.

[16] *Ann. Math.*, n° 162, 2005, p. 1065-1185.

[17] *Forum Math. Pi*, n° 5, 2017, article e2.

[18] *J. High Energy Phys.*, 2019, article 48.

[19] Klarreich (Erica), « Sphere packing solved in higher dimensions », *Quanta Magazine*, 30 mars 2016.

[20] *Nieuw Arch. Wiskd.*, n° 17, 2016, p. 184-192.

[21] *Arithmetic Geometry, Number Theory, and Computation*, Springer, 2021, p. 537-557.

[22] Madore (David), « Sections du diagramme de Voronoï du réseau E_8 », www.madore.org/ david/weblog/d.2017-04-09.2433.html

[23] *Publ. math. IHÉS*, n° 129, 2019, p. 51-81.

[24] Serre (Jean-Pierre), *A Course in Arithmetic*, Springer, 1973.

[25] Thompson (Thomas M.), *From Error-correcting Codes through Sphere Packings to Simple Groups*, Mathematical Association of America, 1983.

[26] *Forhdl. Skand. Naturforsk.*, nº 14, 1892, p. 352-353.

[27] *Ann. Math.*, nº 185, 2017, p. 991-1015.

[28] *The 1-2-3 of Modular Forms*, Springer, 2008, p. 1-103.

Les travaux de Mark Braverman (par Ran Raz)

Mark Braverman a reçu la « médaille de l'abaque » de l'Union mathématique internationale en 2022 pour ses travaux sur la complexité de l'information et pour d'autres travaux complémentaires. Mark est un spécialiste reconnu de la complexité de l'information et ses travaux comptent parmi les plus influents dans ce domaine de recherche. Il a des centres d'intérêt variés et ses travaux clés dans plusieurs autres domaines de recherche ont permis dans certains cas de résoudre des problèmes ouverts en suspens depuis longtemps. Nous décrivons certains de ses travaux en nous concentrant essentiellement sur sa contribution à la complexité de l'information et aux sujets connexes à l'interface de la théorie de la complexité algorithmique et de la théorie de l'information.

1 La complexité de la communication

La complexité de la communication, introduite pour la première fois par Yao [54], est un modèle central de la théorie de la complexité qui étudie la quantité de communication nécessaire pour résoudre un problème lorsque l'entrée du problème est répartie entre deux ou plusieurs ressources.

Dans le modèle distribué à deux joueurs, chacun des deux joueurs reçoit une entrée ; les deux entrées X et Y sont des variables aléatoires tirées selon une loi jointe connue des deux joueurs. L'objectif des joueurs est de résoudre une tâche de communication qui dépend des deux entrées, telle que le calcul d'une fonction $f(X, Y)$, où $f : \{0, 1\}^n \times \{0, 1\}^n \to \{0, 1\}$ est connue des deux joueurs ; X et Y sont des entrées de longueur n bits. Les joueurs communiquent par tours, où à chaque tour l'un des joueurs envoie un message à l'autre joueur. À la fin du protocole, dans l'exemple donné ci-dessus, les deux joueurs doivent connaître la valeur de $f(X, Y)$. Les joueurs peuvent utiliser des chaînes de caractères aléatoires publiques ou privées et se tromper avec une petite probabilité fixée.

La complexité de la communication d'un protocole est le nombre maximal de bits communiqués par les joueurs du protocole, le maxi-

Raz (Ran), « The work of Mark Braverman », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 106-117. DOI 10.4171/ICM2022/214

mum étant pris sur toutes les entrées possibles (dans le support de la loi d'entrée). La complexité de la communication d'une tâche de communication est la complexité de la communication minimale d'un protocole qui résout la tâche avec une probabilité élevée (disons une probabilité supérieure à $\frac{2}{3}$).

2 La complexité de l'information

La complexité de l'information, introduite dans [1, 2, 25], étudie la quantité d'information que deux joueurs doivent révéler sur leurs entrées afin de résoudre une tâche de communication. Le modèle fut motivé par des questions fondamentales de la théorie de l'information sur la compression de la communication, ainsi que par des relations fascinantes avec la complexité de la communication, en particulier pour démontrer des bornes inférieures pour la complexité de la communication et le problème de la somme directe dans la complexité de la communication, un problème qui a une histoire riche et qui a été étudié dans de nombreux travaux et dans des contextes variés.

L'article de Barak, Braverman, Chen et Rao établit une distinction entre les complexités interne et externe de l'information d'un protocole de communication [2]. En gros, la complexité externe d'un protocole, définie pour la première fois dans [25], est la quantité d'information qu'un observateur externe, qui surveille l'exécution du protocole, apprend sur les entrées des joueurs, tandis que la complexité interne d'un protocole, implicite dans [1] et explicitement définie dans [2], est la quantité d'information que les joueurs apprennent sur les entrées de chacun d'entre eux lors de l'exécution du protocole.

Formellement, si M est la transcription du protocole et R la chaîne de caractères aléatoire publique, la complexité externe et la complexité interne de l'information sont définies par

$$\begin{aligned} \mathrm{Ext} &= \mathrm{I}((X, Y); M|R), \\ \mathrm{Int} &= \mathrm{I}(X; M|Y, R) + \mathrm{I}(Y; M|X, R), \end{aligned}$$

où I est la fonction d'information mutuelle conditionnelle. (On sait que les chaînes de caractères aléatoires privées du protocole peuvent être ignorées dans ce cas.)

La complexité (interne ou externe) de l'information d'une tâche de communication est l'infimum de la complexité (interne ou externe) de l'information d'un protocole qui résout la tâche avec une probabilité élevée (disons une probabilité supérieure à $\frac{2}{3}$).

Il n'est pas difficile de démontrer que pour tout protocole (et donc aussi pour toute tâche de communication), la complexité interne de l'information du protocole est au plus égale à la complexité externe de l'information, qui est à son tour au plus égale à la complexité de la communication. Cela a motivé l'étude de la complexité de l'information en tant qu'outil pour démontrer des bornes inférieures pour la complexité de la communication.

La propriété d'additivité, ou propriété de somme directe, est une propriété magnifique et utile de la complexité interne de l'information, qui a motivé sa définition. En gros, la complexité interne de l'information de l'exécution de deux tâches de communication, sur deux paires indépendantes d'entrées, est égale à la somme des complexités internes de l'information des deux tâches. Par conséquent, la complexité interne de l'information de l'exécution de k copies d'une tâche de communication, sur k paires indépendantes d'entrées, est égale à k fois la complexité interne de l'information de la tâche de communication ([1,2,20], qui utilisent les techniques de [43,45]). La propriété de somme directe relie également la complexité de l'information au problème de somme directe dans la complexité de la communication.

Enfin, nous remarquons que dans le cas où les entrées X et Y pour les deux joueurs sont tirées indépendamment, les complexités interne et externe de l'information de n'importe quel protocole sont égales.

La plupart des travaux sur la complexité de l'information ont été regroupés en une théorie dans les travaux de Braverman [2, 6, 7, 20]. Braverman a également défini une variante de la complexité de l'information qui ne dépend pas de la loi *a priori* de l'entrée, ce qui a permis de démontrer que plusieurs définitions possibles sont essentiellement équivalentes [7].

Au départ, il n'était pas certain que la complexité de l'information fût calculable, c'est-à-dire qu'il existât un algorithme qui l'approxime, mais Braverman et Schneider l'ont démontré (pour le cas d'erreur nulle) [23].

3 La compression interactive

Les travaux classiques de Shannon, Fano et Huffman montrent que si un joueur souhaite envoyer un message X à un autre joueur, il lui suffit d'envoyer en moyenne $\lceil H(X) \rceil$ bits, où H désigne la fonction entropie de Shannon [29, 35, 50]. En d'autres termes, la longueur du message peut être compressée à environ H(X), le contenu informatif

du message. Existe-t-il des résultats analogues dans le cadre interactif, lorsque deux joueurs s'engagent dans un protocole de communication interactif ?

Barak, Braverman, Chen et Rao ont commencé à étudier le problème de la compression interactive [2]. Étant donné un protocole de communication dont la complexité de l'information est faible, le protocole peut-il être compressé de manière à ce que le nombre total de bits communiqués par le protocole soit également faible ? Plus formellement, étant donné un protocole de communication Π avec une complexité de la communication C et une complexité (interne ou externe) de l'information $I \ll C$, existe-t-il toujours un protocole équivalent Π' (éventuellement avec une probabilité d'erreur légèrement plus élevée), avec une complexité de la communication significativement plus petite que C (et une complexité de l'information arbitraire) ?

Barak, Braverman, Chen et Rao ont donné deux protocoles de compression différents, l'un pour la complexité interne de l'information et l'autre pour la complexité externe de l'information. Pour la complexité interne de l'information, ils ont démontré que tout protocole de communication Π avec une complexité de la communication C et une complexité interne de l'information I peut être compressé en un protocole équivalent Π', avec une complexité de la communication $O\left(\sqrt{C \cdot I} \cdot \log C\right)$. Pour la complexité externe de l'information, ils ont démontré que tout protocole de communication Π avec une complexité de la communication C et une complexité externe de l'information I peut être compressé en un protocole équivalent Π', avec une complexité de la communication $O(I \cdot \log C)$ [2]. Rappelons que la complexité interne de l'information est toujours inférieure ou égale à la complexité externe de l'information. Il est donc plus facile de compresser la complexité de la communication en une expression proche de la complexité externe de l'information du protocole d'origine.

Ces résultats ont été suivis par de nombreux autres travaux qui ont approfondi le problème de la compression interactive. Braverman et Rao ont démontré que tout protocole de communication à un tour (ou un petit nombre de tours) avec une complexité interne de l'information I peut être compressé en un protocole équivalent avec une complexité de la communication $O(I)$ [20]. Braverman a démontré que tout protocole de communication avec une complexité interne de l'information I peut être compressé en un protocole équivalent avec une complexité de la communication $2^{O(I)}$ [7].

Les travaux révolutionnaires de Kol ont démontré que dans le cas

particulier important où les deux entrées X et Y sont indépendantes, tout protocole de communication avec une complexité interne/externe de l'information I peut être compressé en un protocole équivalent avec une complexité de la communication $O(I^2 \operatorname{polylog}(I))$ [37]. Le point culminant a été atteint par Sherstov qui a amélioré cette dernière complexité de la communication à $O(I \operatorname{polylog}(I))$ [51]. Notons que cette dernière expression ne dépend pas du tout de la complexité de la communication du protocole original et correspond presque à la borne inférieure en $\Omega(n)$. Rappelons que dans le cas où X et Y sont indépendants, les complexités interne et externe de la communication sont égales. En s'appuyant sur ces travaux, Braverman et Kol ont démontré que tout protocole de communication ayant une complexité de la communication C et une complexité externe de l'information I peut être compressé en un protocole équivalent avec une complexité de la communication $\operatorname{poly}(I) \cdot \log\log(C)$ [15].

En ce qui concerne les bornes inférieures, Braverman a proposé un candidat pour une tâche de communication dont la complexité de la communication est exponentiellement plus grande que la complexité (interne ou externe) de l'information [5]. Cette tâche et d'autres tâches de communication ont été analysées dans des travaux ultérieurs, qui ont permis d'établir des écarts exponentiels entre la complexité de la communication et la complexité de l'information [30–32, 42], à savoir des exemples de tâches de communication dont la complexité (interne ou externe) de l'information est I et la complexité de la communication $2^{\Omega(I)}$. En particulier, ces travaux montrent que la compression par Braverman de la complexité de la communication d'un protocole en $2^{O(I)}$ [7] est la meilleure possible, et qu'on ne peut espérer une compression en $\operatorname{poly}(I)$ dans le cas général (comme l'ont obtenu Kol et Sherstov pour le cas particulier d'entrées X et Y indépendantes [37, 51]). À la suite de ces travaux, Braverman et Minzer ont établi des écarts exponentiels entre la complexité interne et externe de l'information [17]. Un important problème ouvert consiste à savoir si la compression en $\operatorname{poly}(I) \cdot \operatorname{polylog}(C)$, où I est la complexité interne de l'information, est possible dans le cas général [11]. Comme on l'a décrit ci-dessus, les meilleures compressions connues aujourd'hui sont les compressions en $O\left(\sqrt{C \cdot I} \cdot \log C\right)$ [2] et $2^{O(I)}$ [7].

Dans chacun des protocoles de compression mentionnés ci-dessus, les deux joueurs parviennent à échantillonner ensemble, avec une faible communication, une transcription du protocole original, de sorte que la transcription est échantillonnée (approximativement) à partir de la

loi de probabilité correcte des transcriptions et que les deux joueurs s'accordent sur la même transcription avec une forte probabilité. L'une des difficultés réside dans le fait qu'aucun des joueurs ne connaît la loi de probabilité correcte des transcriptions.

Pour illustrer la saveur des techniques utilisées dans ces résultats, nous énonçons un théorème remarquable issu des travaux de Braverman et Rao [20] :

Théorème 1. *Supposons que le joueur 1 connaisse une loi de probabilité P et que le joueur 2 connaisse une loi Q sur le même ensemble fini U. Pour tout $\varepsilon > 0$, il existe un protocole de communication à jeton public qui utilise un nombre moyen de*

$$\mathrm{D}(\mathrm{P}\|\mathrm{Q}) + 2\log(1/\varepsilon) + \mathrm{O}\Big(\sqrt{\mathrm{D}(\mathrm{P}\|\mathrm{Q})} + 1\Big)$$

bits de communication, où $\mathrm{D}(\mathrm{P}\|\mathrm{Q}) = \sum_x \mathrm{P}(x)\log(\mathrm{P}(x)/\mathrm{Q}(x))$ est la divergence de Kullback-Leibler, de telle sorte qu'à la fin du protocole, le joueur 1 délivre un élément a distribué selon P et le joueur 2 délivre un élément b tel que pour tout $x \in \mathrm{U}$, $\mathbb{P}(b = x \,|\, a = x) > 1 - \varepsilon$.

4 La somme directe

L'une des premières motivations pour étudier la complexité de l'information est venue des relations avec le problème de la somme directe dans la complexité de la communication. Le problème de la somme directe pose la question de savoir quelles sont les relations entre la complexité de la communication d'une tâche de communication et la complexité de la communication de l'exécution de k copies de la même tâche sur k entrées choisies indépendamment.

Soit T une tâche de communication. Pour tout k, soit T^k la tâche qui consiste à effectuer k copies de la tâche T, sur k entrées choisies indépendamment selon la loi de probabilité des entrées de T, en permettant de se tromper sur chaque copie avec la même probabilité d'erreur que celle autorisée pour la tâche T. La complexité de la communication amortie d'une tâche T est définie par

$$\lim_{k\to\infty} \frac{\mathrm{CC}(\mathrm{T}^k)}{k}$$

où CC désigne la complexité de la communication.

Braverman et Rao ont démontré que la complexité de la communication amortie de toute tâche T est exactement égale à sa complexité

interne de l'information [20] (voir également [41]). Ce résultat surprenant établit un lien entre le problème de la somme directe dans la complexité de la communication et le problème de la compression interactive.

On pourrait penser *a priori* que la complexité de la communication amortie d'une tâche devrait toujours être proche de sa complexité de la communication. Cependant, en utilisant l'équivalence de Braverman et Rao entre la complexité de la communication amortie et la complexité interne de l'information, les écarts exponentiels mentionnés ci-dessus entre la complexité de la communication et la complexité interne de l'information impliquent également des écarts exponentiels entre la complexité de la communication et la complexité de la communication amortie, ce qui montre qu'il existe des tâches de communication avec une complexité de la communication C et une complexité de la communication amortie $O(\log C)$ [30, 31, 42]. Cela montre qu'une propriété de somme directe forte ne s'applique pas à la complexité de la communication.

Inversement, chacun des protocoles de compression mentionnés ci-dessus, en termes de complexité interne de l'information, implique une borne inférieure sur la complexité de la communication amortie. Par exemple, les protocoles de compression de Kol et Sherstov [37, 51] impliquent pour le cas particulier où X et Y sont indépendants que la complexité de la communication et la complexité de la communication amortie sont essentiellement égales (à une fonction polylogarithmique près), tandis que le protocole de compression de Braverman [7] implique que la complexité de la communication amortie est au moins logarithmique en la complexité de la communication.

Les travaux complémentaires de Braverman, Rao, Weinstein et Yehudayof [22] et Braverman et Weinstein [24] montrent que si un protocole tente de résoudre T^k avec une complexité de la communication significativement plus petite que k fois la complexité de la communication amortie de T, alors la probabilité de succès du protocole est exponentiellement petite.

5 Complexité de la communication de l'intersection d'ensembles

L'intersection d'ensembles, ou la disjonction d'ensembles, est un problème central de la complexité de la communication. Dans ce problème, chacun des deux joueurs (ou plus) reçoit un vecteur dans $\{0, 1\}^n$ et leur but est de déterminer s'il existe une coordonnée $i \in$

$[\![1, n]\!]$ où ils ont tous les deux (ou tous) 1. Ce problème simple a inspiré de nombreux progrès dans les domaines de la complexité de la communication et de la complexité de l'information.

On sait depuis 1987 que la complexité de la communication probabiliste de l'intersection d'ensembles est au moins $\Omega(n)$ [36, 45]. Le principal résultat de l'article de Bar-Yossef, Jayram, Kumar et Sivakumar, l'un des articles à l'origine du domaine de recherche de la complexité de l'information, était une nouvelle démonstration de la borne inférieure en $\Omega(n)$ pour l'intersection d'ensembles, en utilisant la complexité de l'information [1]. Cette démonstration a été l'une des principales motivations pour étudier la complexité de l'information.

Braverman a utilisé la complexité de l'information pour étudier de nombreux aspects supplémentaires de la complexité de la communication de l'intersection d'ensembles.

Alors que l'on savait que la complexité de la communication probabiliste de l'intersection d'ensembles était en $\Theta(n)$ [1, 36, 45], Braverman, Garg, Pankratov et Weinstein ont étudié la complexité de l'information de la fonction booléenne ET. À partir de cette analyse, ils ont trouvé la constante exacte dans l'expression $\Theta(n)$, c'est-à-dire qu'ils ont calculé exactement la complexité de la communication probabiliste de l'intersection d'ensembles, y compris les termes du second ordre [14].

Braverman et Moitra ont étudié des protocoles de communication pour l'intersection d'ensembles qui obtiennent un avantage d'au moins ε par rapport à une supposition aléatoire. Ils ont démontré une borne inférieure étroite $\Omega(\varepsilon n)$ pour la complexité de la communication d'un tel protocole [18], alors que les démonstrations précédentes n'impliquaient qu'une borne inférieure $\Omega(\varepsilon^2 n)$. À partir de leur borne inférieure améliorée, ils ont obtenu comme application des bornes inférieures pour la taille des programmes linéaires.

Braverman, Ellen, Oshman, Pitassi et Vaikuntanathan [10] et Braverman et Oshman [19] ont utilisé la complexité de l'information pour démontrer des bornes inférieures étroites pour la complexité de la communication de l'intersection d'ensembles avec plus de deux joueurs. Braverman, Garg, Kun-Ko, Mao et Touchette ont utilisé une variante quantique de la complexité de l'information pour démontrer des bornes inférieures pour la complexité de la communication quantique de l'intersection d'ensembles avec un nombre limité de tours [13].

6 Répétition parallèle de jeux à deux joueurs

La complexité de l'information est étroitement liée à l'étude de la répétition parallèle des jeux à deux joueurs. Les deux domaines font un usage substantiel de la théorie de l'information, mais le lien est plus profond ; les deux domaines utilisent de nombreuses idées, intuitions, définitions, outils et techniques similaires (tels que la sous-additivité de l'entropie, les événements de rupture de corrélation et l'échantillonnage corrélé).

Dans un jeu à deux joueurs, un arbitre tire des questions (x, y) selon une loi (connue publiquement) et envoie x au premier joueur et y au second joueur. Le premier joueur répond par $a = a(x)$ et le second par $b = b(y)$ (sans communiquer entre eux). Les joueurs gagnent conjointement si un prédicat (connu publiquement) $\mathrm{V}(x, y, a, b)$ est vérifié. La valeur du jeu est la probabilité maximale de succès que les joueurs peuvent atteindre, le maximum étant pris sur tous les protocoles $a = a(x)$ et $b = b(y)$.

En gros, une répétition parallèle d'un jeu à deux joueurs est un jeu dans lequel les joueurs essaient de gagner simultanément n copies du jeu original. Plus précisément, l'arbitre pose des questions $x = (x_1, \ldots, x_n)$ et $y = (y_1, \ldots, y_n)$, où chaque couple (x_i, y_i) est choisi indépendamment selon la loi initiale. Les joueurs répondent par $a = (a_1, \ldots, a_n) = a(x)$ et $b = (b_1, \ldots, b_n) = b(y)$. Les joueurs gagnent s'ils gagnent simultanément sur toutes les coordonnées, c'est-à-dire si pour tout i, $\mathrm{V}(x_i, y_i, a_i, b_i)$ est vérifié.

Le théorème de répétition parallèle stipule que pour tout jeu à deux joueurs dont la valeur est inférieure à 1, la valeur du jeu répété en parallèle n fois décroît exponentiellement vite avec n [43]. Le théorème de répétition parallèle et d'autres résultats sur la répétition parallèle de jeux à deux joueurs ont de nombreuses applications dans le domaine de la complexité algorithmique et dans d'autres domaines de recherche.

Bien que l'on sache depuis longtemps que la répétition parallèle réduit la valeur des jeux à deux joueurs de manière exponentielle, le taux exact de décroissance exponentielle n'était pas connu lorsque la valeur du jeu était déjà faible, pour commencer. (Une analyse rigoureuse pour les jeux de faible valeur n'était connue que pour le cas particulier des jeux de projection [27].)

Braverman et Garg ont résolu ce problème. Ils ont démontré que si la valeur du jeu est $v < 1/2$ et si la longueur des réponses est s, alors la valeur du jeu répété en parallèle n fois est au plus $v^{\Omega(n \log(1/v)/s)}$ [12]. On

ne connaissait auparavant qu'une borne en $2^{-\Omega(n/s)}$ [43].

7 Théorie des codes interactifs

Le célèbre article de Shannon publié en 1948 sur la théorie mathématique de la communication est à l'origine (parmi de nombreuses autres contributions célèbres) du domaine des codes correcteurs. Supposons qu'un joueur veuille envoyer un message de longueur n bits à un autre joueur, mais que le seul canal disponible soit bruyant et modifie chaque bit envoyé avec une probabilité constante (inférieure à $1/2$). Shannon a démontré que le joueur peut envoyer un message d'une longueur de $O(n)$ bits sur un canal bruyant de telle sorte que le message original puisse être récupéré à partir de ce message avec une probabilité élevée et sans erreur [50]. Existe-t-il des résultats analogues dans le cadre interactif, lorsque deux joueurs s'engagent dans un protocole de communication interactif ?

Cette question a été posée et résolue pour la première fois par Schulman en 1992. Schulman a montré comment traduire tout protocole de communication interactif en un protocole équivalent résistant au bruit qui fonctionne sur un canal bruyant avec seulement un surcoût constant dans la complexité de la communication (même lorsque le bruit est choisi de manière antagoniste) [47–49]. Ces résultats ont donné naissance à la théorie des codes interactifs, l'étude de la manière d'exécuter un protocole de communication interactif de manière fiable en présence de bruit.

En 2011, Braverman et Rao ont commencé à étudier la question de la fraction maximale d'erreurs qui peut être récupérée dans un protocole interactif. Alors que les travaux de Schulman ne permettaient de récupérer qu'une fraction d'erreurs bornée par $1/240$, Braverman et Rao ont montré comment récupérer une fraction d'erreurs de $1/4 - \varepsilon$ lorsque la taille de l'alphabet de codage est une certaine constante, et une fraction d'erreurs de $1/8 - \varepsilon$ lorsque la taille de l'alphabet de codage est égale à 2. Le résultat est valable même dans le cas antagoniste au prix d'une augmentation de la complexité de la communication du protocole d'un facteur constant seulement [21]. (La fraction d'erreurs de $1/8 - \varepsilon$ pour un alphabet de codage de taille 2 a été récemment améliorée à une fraction optimale de $1/6 - \varepsilon$ [28,34].)

Ce travail de Braverman et Rao a suscité un regain d'intérêt pour la théorie des codes interactifs et a inspiré de nombreux travaux complémentaires. Braverman a étudié d'autres aspects de la théorie des

codes interactifs dans de nombreux travaux ultérieurs. Par exemple, Braverman et Efremenko ont étudié le décodage de listes pour la communication interactive [8] tandis que Braverman, Efremenko, Gelles et Haeupler ont démontré que le codage à taux constant pour la communication interactive multipartite était impossible [9].

8 Des bornes inférieures pour les circuits à profondeur bornée

Les circuits booléens à profondeur bornée font partie des sous-classes les plus importantes de circuits booléens. Ils ont été étudiés de manière approfondie dans de nombreux ouvrages. Ils jouent un rôle central dans de nombreux sous-domaines de la théorie de la complexité ainsi que dans l'analyse des fonctions booléennes. En gros, un circuit booléen calcule une fonction booléenne de n variables binaires d'entrée en utilisant des portes ET, OU et NON, où le nombre d'entrées des portes ET et OU n'est pas borné. La taille du circuit est le nombre de fils qu'il contient et la profondeur du circuit est la longueur du plus long chemin direct entre une variable d'entrée et la sortie (sans compter les portes NON).

En 1990, Linial et Nisan ont conjecturé que les circuits de taille m et de profondeur d ne peuvent pas faire la distinction entre la loi uniforme sur les entrées et toute loi indépendante par k-uplets sur les entrées avec $k \geqslant (\log m)^{d-1}$ [40]. Cette conjecture signifie qu'un circuit de profondeur bornée ne peut pas reconnaître une structure globale tant qu'elle n'est pas accompagnée d'une structure locale. Il s'agissait d'une conjecture importante, mais il y a eu très peu de progrès pendant de nombreuses années. La conjecture n'avait été démontrée que pour les formes normales disjonctives (c'est-à-dire pour les circuits de profondeur 2) [3, 46].

En 2009, Braverman a démontré que les circuits de taille m et de profondeur d ne peuvent pas faire la distinction entre la loi uniforme sur les entrées et toute loi indépendante par k-uplets sur les entrées avec $k \geqslant (\log m)^{\mathrm{O}(d^2)}$ [4]. Ce résultat démontre qualitativement la conjecture avec des paramètres un peu plus faibles.

Pour démontrer ce résultat, Braverman combine brillamment deux types différents d'approximation de circuits à profondeur bornée par des polynômes de bas degré. Le premier type, celui de Razborov et Smolensky [44,52], donne un polynôme qui est égal à la fonction calculée par le circuit presque partout, mais qui peut en être très différent sur une petite fraction des entrées. Braverman observe que la différence

entre la fonction calculée par le circuit et le polynôme d'approximation peut elle-même être calculée par un circuit à profondeur bornée. Il approxime ensuite cette différence par un polynôme de faible degré en utilisant un autre type d'approximation, l'approximation donnée par Linial, Mansour et Nisan [39], qui approxime un circuit à profondeur bornée par un polynôme de faible degré qui est proche de la fonction calculée par le circuit en moyenne. Le résultat final est un polynôme de faible degré qui approxime si bien le circuit original que la preuve triviale que les polynômes de faible degré ne peuvent pas faire la distinction entre la loi uniforme et les lois indépendantes par k-uplets (avec k plus grand ou égal au degré du polynôme) fonctionne [4].

Depuis que Braverman a publié ses travaux, ceux-ci ont été améliorés et sont devenus plus importants de deux manières. Tout d'abord, les travaux révolutionnaires de Tal [53] ont amélioré l'approximation donnée par Linial, Mansour et Nisan [39]. En introduisant les nouveaux paramètres dans la démonstration de Braverman, il a obtenu un résultat amélioré : les circuits de taille m et de profondeur d ne peuvent pas distinguer entre la loi uniforme sur les entrées et n'importe quelle loi indépendante par k-uplets sur les entrées avec $k \geqslant (\log m)^{O(d)}$ [53]. Cela nous rapproche encore plus de la démonstration de la conjecture originale. En outre, Chattopadhyay et Zuckerman ont utilisé ces résultats dans leur construction révolutionnaire d'extracteurs explicites à deux sources [26].

9 Constante de Grothendieck et borne de Krivine

Grothendieck a démontré en 1953 qu'il existe une constante strictement positive $K \in \mathbb{R}$ telle que, pour toute matrice réelle $(a_{ij})_{i\in[m],j\in[n]}$ de taille $m \times n$,

$$\max_{\{X_i\},\{Y_j\}} \sum_{i,j} a_{ij}\langle X_i, Y_j\rangle \leqslant K \cdot \max_{\{x_i\},\{y_j\}} \sum_{i,j} a_{ij}x_i y_j,$$

où X_i et Y_j (dans le premier membre) sont des vecteurs unitaires dans $\mathbb{R}^{m+n}$, tandis que x_i et y_j (dans le second membre) sont dans $\{-1, 1\}$ [33]. On appelle « constante de Grothendieck » la plus petite valeur de K qui vérifie cette inégalité.

Il s'agit d'un théorème important qui a des applications dans plusieurs domaines. En informatique, la constante de Grothendieck peut être considérée comme l'écart d'intégrité entre un maximum obtenu sur les valeurs dans $\{-1, 1\}$ dans le second membre, qui est souvent

souhaitable mais difficile à calculer, et le maximum obtenu sur les vecteurs unitaires dans le premier membre, qui peut être calculé en temps polynomial.

On ne connaît toujours pas la valeur exacte de la constante de Grothendieck. Krivine a démontré en 1979 que la constante de Grothendieck était inférieure ou égale à $\frac{\pi}{2\ln(1+\sqrt{2})}$ et a conjecturé qu'il s'agissait d'une égalité [38]. Cette conjecture a été réfutée par Braverman, Makarychev, Makarychev et Naor [16].

Financement. Soutenu par la collaboration Simons sur les algorithmes et la géométrie, par une bourse de recherche Simons et par les subventions de la Fondation nationale des sciences nº CCF-1714779 et CCF-2007462.

Bibliographie

[1] *J. Comput. System Sci.*, nº 68-4, 2004, p. 702-732.

[2] *SIAM J. Comput.*, nº 42-3, 2013, p. 1327-1363.

[3] *SIAM J. Comput.*, nº 38-6, 2009, p. 2220-2272.

[4] *J. ACM*, nº 57-5, 2010, p. 28:1-28:10.

[5] *51th Annual Allerton Conference on Communication, Control, and Computing*, IEEE, 2013, p. 8-12.

[6] *Proceedings of the International Congress of Mathematicians 2014*, Séoul, Kyung Moon SA, 2014, p. 535-559.

[7] *SIAM J. Comput.*, nº 44-6, 2015, p. 1698-1739.

[8] *SIAM J. Comput.*, nº 46-1, 2017, p. 388-428.

[9] *J. ACM*, nº 65-1, 2018, p. 4:1-4:41.

[10] *Annual Symposium on Foundations of Computer Science*, IEEE, 2013, p. 668-677.

[11] *9th Innovations in Theoretical Computer Science Conference*, Schloss Dagstuhl, Leibniz-Zentrum für Informatik, 2018, p. 11:1-11:13.

[12] *Proceedings of the 2015 ACM Symposium on Theory of Computing*, 2015, p. 335-340.

[13] *SIAM J. Comput.*, nº 47-6, 2018, p. 2277-2314.

[14] *Proceedings of the 2013 ACM Symposium on Theory of Computing*, 2013, p. 151-160.

[15] *Proceedings of the 2018 ACM Symposium on Theory of Computing*, ACM, 2018, p. 964-977.

[16] *Annual Symposium on Foundations of Computer Science*, IEEE, 2011, p. 453-462.

[17] *Proceedings of the 2021 ACM Symposium on Theory of Computing*, 2021, p. 248-258.

[18] *Proceedings of the 2013 ACM Symposium on Theory of Computing*, 2013, p. 161-170.

[19] *Annual Symposium on Foundations of Computer Science*, IEEE, 2017, p. 144-155.

[20] *IEEE Trans. Inf. Theory*, nº 60-10, 2014, p. 6058-6069.

[21] *IEEE Trans. Inf. Theory*, nº 60-11, 2014, p. 7248-7255.

[22] *Annual Symposium on Foundations of Computer Science*, IEEE, 2013, p. 746-755.

[23] *43rd International Colloquium on Automata, Languages, and Programming*, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, p. 87:1-87:10.

[24] *Proceedings of the 2015 ACM Symposium on Theory of Computing*, 2015, p. 341-350.

[25] *Annual Symposium on Foundations of Computer Science*, IEEE, 2001, p. 270-278.

[26] *Proceedings of the 2016 ACM Symposium on Theory of Computing*, 2016, p. 670-683.

[27] *Proceedings of the 2014 ACM Symposium on Theory of Computing*, 2014, p. 624-633.

[28] *Annual Symposium on Foundations of Computer Science*, IEEE, 2020, p. 470-481.

[29] Fano (R. M.), *The Transmission of Information*, Massachusetts Institute of Technology, Research Laboratory of Electronics, 1949.

[30] *Annual Symposium on Foundations of Computer Science*, IEEE, 2014, p. 176-185.

[31] *J. ACM*, nº 63-5, 2016, p. 46:1-46:31.

[32] *Proceedings of the 2016 ACM Symposium on Theory of Computing*, 2016, p. 977-986.

[33] *Bol. Soc. Mat. São Paulo*, nº 8, 1953, p. 1-79.

[34] *Proceedings of the 2022 ACM Symposium on Theory of Computing*, 2022, p. 948-961.

[35] *Proc. IRE*, nº 40-9, 1952, p. 1098-1101.

[36] *SIAM J. Discrete Math.*, nº 5-4, 1992, p. 545-557.

[37] *Proceedings of the 2016 ACM Symposium on Theory of Computing*, 2016, p. 987-998.

[38] *Adv. Math.*, nº 31-1, 1979, p. 16-30.

[39] *J. ACM*, nº 40-3, 1993, p. 607-620.

[40] *Combinatorica*, nº 10-4, 1990, p. 349-365.

[41] *IEEE Trans. Inf. Theory*, nº 59-7, 2013, p. 4071-4094.

[42] *Theory Comput.*, nº 14-1, 2018, p. 1-29.

[43] *SIAM J. Comput.*, nº 27-3, 1998, p. 763-803.

[44] *Math. Notes Acad. Sci. USSR*, nº 41-4, 1987, p. 333-338.

[45] *Theoret. Comput. Sci.*, nº 106-2, 1992, p. 385-390.

[46] *ACM Trans. Comput. Theory*, nº 1-1, 2009, p. 3:1-3:5.

[47] *Annual Symposium on Foundations of Computer Science*, IEEE, 1992, p. 724-733.

[48] *Proceedings of the 2016 ACM Symposium on Theory of Computing*, 1993, p. 747-756.

[49] *IEEE Trans. Inf. Theory*, nº 42-6, 1996, p. 1745-1756.

[50] Shannon (Claude E.), *A Mathematical Theory of Communication*, Bell Syst. Tech. J., 1948.

[51] *SIAM J. Comput.*, nº 47-2, 2018, p. 367-419.

[52] *Proceedings of the 1987 ACM Symposium on Theory of Computing*, 1987, p. 77-82.

[53] *Computational Complexity Conference*, Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017, p. 15:1-15:31.

[54] *Proceedings of the 1979 ACM Symposium on Theory of Computing*, 1979, p. 209-213.

Les travaux de Barry Mazur (par Henri Darmon)

Barry Mazur reçoit la médaille Chern[1] *en 2022 « pour ses découvertes profondes en topologie, en géométrie arithmétique et en théorie des nombres, ainsi que pour son rôle moteur et sa générosité dans la formation de la prochaine génération ». Cet éloge passe en revue quelques-uns des faits marquants de la remarquable carrière mathématique de Mazur.*

Barry Mazur est né en 1937 à New York. Après avoir terminé ses études au lycée scientifique du Bronx en 1954, il a achevé ses études de premier cycle à l'institut de technologie du Massachusetts en deux ans seulement, et son doctorat à l'université de Princeton en deux ans supplémentaires. Au cours de son doctorat, il a également passé un semestre à Paris, où il a assisté notamment aux séminaires de Cartan et Chevalley. Après un séjour d'un an à l'Institut d'études avancées, il a rejoint le département de mathématiques de Harvard en 1959, d'abord en tant que membre de la société des boursiers de Harvard, et actuellement en tant que professeur sur la chaire Gerhard-Gade.

Au cours d'une carrière remarquable qui s'étend sur plus de six décennies, rien qu'à Harvard, Barry Mazur a profondément influencé les perspectives scientifiques de générations de doctorants, postdoctorants et chercheurs confirmés. Il a façonné le paysage moderne de la théorie des nombres en s'attaquant avec succès aux problèmes les plus difficiles dans ce domaine, en jetant les bases de théories importantes et en initiant des légions de disciples à de nouvelles perspectives fécondes. Ses réalisations scientifiques le placent assurément parmi les plus grands mathématiciens du XX^e siècle. Le texte qui suit aborde dans un ordre approximativement chronologique quelques-uns des sujets sur lesquels Barry Mazur a eu un impact déterminant.

Darmon (Henri), « The work of Barry Mazur », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 118-141. DOI 10.4171/ICM2022/217

1. NDT. Le nom s'écrit « Chén » en pinyin et « Tchen » selon le système de transcription de l'École française d'Extrême-Orient.

1 Topologie géométrique et différentielle

Références : [1–19].

Les premières contributions de Barry Mazur ont été réalisées dans le domaine de la topologie géométrique et de la géométrie différentielle. Sa thèse de doctorat de 1959 à Princeton [4] a fait sensation en démontrant la conjecture de Schoenflies généralisée, une généralisation en dimension supérieure du théorème de Jordan pour les courbes du plan. Cette conjecture affirme qu'une $(n-1)$-sphère S plongée dans la n-sphère S^n d'une manière qui se prolonge en un plongement d'un petit épaississement de S peut être appliquée sur la $(n-1)$-sphère standard par un homéomorphisme de S^n [4–6]. La nécessité de certaines hypothèses de régularité sur le plongement est illustrée par des contre-exemples bien connus comme la sphère cornue d'Alexander. L'une des idées ingénieuses de Mazur dans la démonstration est l'« astuce » éponyme, qui montre que la somme connexe de deux nœuds ou variétés non triviaux est nécessairement non triviale. L'argument, d'une simplicité séduisante, est basé sur le fait que les sommes connexes infinies ont un sens rigoureux dans le cadre des « nœuds sauvages » ; si K_1 et K_2 sont des nœuds ou des variétés pour lesquels $K_1 + K_2$ est trivial, alors

$$K_1 = K_1 + (K_2 + K_1) + (K_2 + K_1) + \cdots = (K_1 + K_2) + (K_1 + K_2) + \cdots = 0$$

et de même pour K_2. Mazur a reçu avec Morton Brown le prix Oswald-Veblen de la Société américaine de mathématiques en 1966 pour son travail sur la conjecture de Schoenflies généralisée.

Parmi d'autres notions clés, Mazur a également découvert, indépendamment et à peu près en même temps que Valentin Poénaru, ce que l'on appelle aujourd'hui dans la littérature les « variétés de Mazur » ou les « variétés de Poénaru-Mazur » [7] : des variétés compactes de dimension 4, contractiles et lisses dont les bords ne sont pas difféomorphes à la boule standard de dimension 4.

L'article de Mazur [15] sur les systèmes dynamiques, en collaboration avec Michael Artin, étudie l'espace F des applications k fois différentiables d'une variété différentielle compacte M dans elle-même, muni de la topologie (C^k) appropriée, et démontre qu'il existe une partie dense de F constituée d'applications dont le nombre de points périodiques isolés de période n croît au plus exponentiellement avec n. La démonstration s'obtient en invoquant un théorème d'approximation de Nash pour se ramener à un énoncé analogue pour les variétés

algébriques réelles, qui peut alors être abordé avec les méthodes de la théorie de l'intersection des cycles algébriques.

2 Géométrie algébrique

Références : [15, 20–29].

Avec son mélange attrayant de méthodes différentielles et algébriques, [15] a marqué un élargissement progressif des centres d'intérêt mathématiques de Mazur à la géométrie algébrique, à une époque où le sujet connaissait un profond renouveau sous l'impulsion de l'école de Grothendieck. C'est au cours de cette période, dans les années soixante et au début des années soixante-dix, que Mazur a produit un certain nombre de travaux fondamentaux en géométrie algébrique, nourris par des visites régulières à l'Institut des hautes études scientifiques (IHÉS).

Ses articles [20] et [21] étudient l'interaction entre l'endomorphisme de Frobenius et la filtration de Hodge sur la cohomologie de de Rham d'une variété V sur $\mathbb{Q}_p$ qui admet un modèle lisse sur $\mathbb{Z}_p$. Ils établissent la fondamentale « inégalité de Mazur », conjecturée à l'origine par Nick Katz [132], qui affirme que « le polygone de Newton se trouve au-dessus du polygone de Hodge ». Le polygone de Newton mesure les pentes, ou les valuations en p, des valeurs propres de l'endomorphisme de Frobenius agissant sur la i-ième cohomologie cristalline de V, ou de manière équivalente, du relèvement canonique de Frobenius à la cohomologie de de Rham de V sur $\mathbb{Q}_p$. Le polygone de Hodge code les dimensions des quotients successifs de cette cohomologie de de Rham relative à la filtration de Hodge. Ces derniers invariants se calculaient classiquement par des méthodes transcendantes complexes, en étudiant la décomposition de Hodge sur la cohomologie de de Rham des variétés sur $\mathbb{C}$. L'inégalité de Mazur décrit une caractéristique fondamentale du comportement de la cohomologie algébrique de de Rham d'une variété par « réduction modulo p », et fournit des informations p-adiques subtiles sur les fonctions zêta des variétés sur des corps finis de caractéristique p.

Le traité de Mazur et Messing [22] sur la cohomologie cristalline représente une contribution fondamentale à l'étude des théories de cohomologie p-adiques. Ce sujet s'est progressivement imposé comme un outil puissant pour comprendre les représentations p-adiques des groupes de Galois des corps p-adiques qui dérivent de la cohomologie étale des variétés algébriques. Il s'est impétueusement développé au

cours des dernières décennies et a acquis une importance croissante en théorie des nombres, notamment dans la théorie des motifs et dans le programme de Langlands.

Certaines des contributions ultérieures de Mazur qui englobent des perspectives de la théorie de Hodge p-adique seront évoquées plus en détail ci-dessous, notamment dans la section 9 avec sa célèbre conjecture avec Jean-Marc Fontaine qui caractérise les représentations galoisiennes globales p-adiques réalisées dans la cohomologie étale p-adique des variétés sur les corps de nombres. La théorie des périodes p-adiques joue également un rôle clé dans l'extension aux formes modulaires de poids supérieur de la définition de l'invariant $\mathscr{L}$ de Mazur, John Tate et Jeremy Teitelbaum qui apparaît dans les termes principaux de certaines fonctions L p-adiques en présence d'un « zéro exceptionnel » (voir section 8).

Une autre réalisation notable de cette période est l'article [28] avec M. Artin qui pose les bases d'une théorie de l'homotopie pour les schémas, basée sur la topologie étale qui avait été introduite moins de dix ans auparavant et qui a depuis joué un rôle central dans la géométrie arithmétique.

3 Topologie arithmétique

Référence : [30].

Dans sa transition progressive de la topologie et de la géométrie vers la théorie des nombres, Mazur semble avoir été guidé et inspiré par une analogie suggestive entre les nœuds et les nombres premiers.

Un nœud est une copie du cercle S^1 plongée dans une 3-sphère S^3. De nombreux invariants de nœuds découlent de l'étude du groupe fondamental du complémentaire du nœud. Il existe un parallèle magnifique et séduisant entre ce complémentaire du nœud et le complémentaire d'un nombre premier dans le schéma $\mathrm{Spec}(\mathbb{Z})$. En effet, ce dernier espace partage certaines des mêmes propriétés homologiques que S^3 dans la mesure où la partie intéressante de sa cohomologie est concentrée au degré 3, alors que $\mathrm{Spec}(\mathbb{F}_p)$ se comporte comme un cercle puisque son groupe fondamental est (topologiquement pro-) cyclique.

La recherche de cette analogie conduit à un dictionnaire fascinant entre la théorie des nombres et la théorie des nœuds, dans lequel la réciprocité quadratique résonne avec la symétrie de l'enlacement de deux nœuds, et les symboles de résidus quadratiques supérieurs de

Rédei peuvent être envisagés comme des analogues de l'enlacement supérieur de configurations de nœuds comme les célèbres anneaux borroméens, les deux notions étant des manifestations de produits de Massey supérieurs.

Le manuscrit non publié mais très influent de Mazur [30] enrichit le lexique de la théorie des nombres et de la théorie des nœuds en expliquant le parallèle entre le polynôme d'Alexander d'un nœud et la description algébrique conjecturale d'Iwasawa de la fonction zêta p-adique de Kubota-Leopoldt en tant que série entière caractéristique d'un certain module d'Iwasawa construit à partir de groupes des classes d'idéaux de corps cyclotomiques pour une puissance de p. Le module d'Iwasawa en question peut être identifié par la théorie globale des corps de classes avec la (pro-p-)extension abélienne maximale de l'extension abélienne maximale de $\mathbb{Q}$ ramifiée seulement en p. Elle peut alors être comprise comme le second terme de l'objet gradué associé à une filtration naturelle sur le groupe fondamental (la complétion prorésoluble du groupe fondamental) du complémentaire de $\mathrm{Spec}(\mathbb{F}_p)$ dans $\mathrm{Spec}(\mathbb{Z})$. L'interprétation d'Iwasawa de la fonction zêta p-adique ressemble au polynôme d'Alexander d'un nœud K, qui code le polynôme caractéristique d'un générateur de l'homologie du complémentaire du nœud agissant sur le terme suivant de l'objet gradué associé à la filtration de $\pi_1(S^3 - K)$ donnée par sa suite centrale descendante.

La riche analogie entre les nœuds et les nombres premiers qui a guidé Mazur dans sa transition de la topologie à la théorie des nombres a par la suite donné naissance à un tout nouveau domaine, connu sous le nom de topologie arithmétique, qui est élégamment décrit dans le récent manuel de Masanori Morishita [138] (voir également [146] pour d'autres manifestations frappantes de l'analogie).

4 Sous-groupes de torsion des courbes elliptiques

Références : [32–38, 122].

L'étude approfondie et systématique des points de torsion rationnels sur les courbes elliptiques, réalisée au cours de la décennie 1975-1985, fait partie des contributions marquantes de Mazur à la théorie des nombres.

Une courbe elliptique sur un corps F est une courbe projective lisse E de genre un sur F munie d'un point rationnel distingué $O \in E(F)$. Ce qui rend ces courbes particulièrement riches d'un point de vue arithmétique,

c'est qu'elles sont dotées d'une structure de groupe algébrique projectif. En particulier, l'ensemble $E(\mathbb{Q})$ des points rationnels sur une courbe elliptique sur $\mathbb{Q}$ est un groupe abélien, qui est de type fini d'après le théorème de Mordell-Weil. Il est donc isomorphe à

$$E(\mathbb{Q}) = \mathbb{Z}^r \times T\,,$$

où T est un groupe fini, appelé sous-groupe de torsion de E sur $\mathbb{Q}$. Le célèbre théorème de Mazur [36] énumère toutes les possibilités pour les groupes T qui peuvent apparaître de cette manière :

Théorème 1. *Le sous-groupe de torsion* T *d'une courbe elliptique sur* $\mathbb{Q}$ *ne peut être isomorphe qu'à l'un des quinze groupes suivants :*

$\mathbb{Z}/n\mathbb{Z}$ *avec* $1 \leqslant n \leqslant 10$ *ou* $n = 12$, $\quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ *avec* $n = 2, 4, 6$ *ou* 8.

Ce résultat frappant a été anticipé par le géomètre italien Beppo Levi [142] en 1908. Il est devenu plus largement connu sous la forme d'une conjecture précise formulée par Andrew Ogg [139] et constitue la toile de fond d'un domaine de recherche actif auquel des mathématiciens comme Kamienny [130], Merel [135] et bien d'autres ont apporté d'importantes contributions par la suite. En effet, l'étude des points rationnels sur les courbes modulaires reste un terrain de recherche vivant auquel une variété d'approches fondées sur les idées pionnières de [36] ont été appliquées : voir par exemple [127,128,133,134,136,137]...

Au-delà de la nature attrayante de l'énoncé final « pour lui-même », les perspectives que Mazur a introduites dans le sujet afin de démontrer le théorème 1 ont également eu un impact considérable sur d'autres développements connexes. L'énoncé et la démonstration du théorème 1 sont des ingrédients indispensables à la démonstration de la modularité des courbes elliptiques et du dernier théorème de Fermat, comme nous l'expliquerons plus en détail dans les sections 5, 6 et 10.

Dans un article ultérieur [37], Mazur a également classifié les nombres premiers N pour lesquels il existe des courbes elliptiques sur $\mathbb{Q}$ possédant un sous-groupe rationnel d'ordre N, c'est-à-dire une isogénie non triviale de degré N définie sur $\mathbb{Q}$, simplifiant par la même occasion sa démonstration précédente du théorème 1 :

Théorème 2. *Soit* N *un nombre premier tel qu'une courbe elliptique admette une isogénie de degré* N *définie sur* $\mathbb{Q}$. *Alors* $N = 2, 3, 5, 7, 13$ *(avec une infinité de* E *possibles pour chaque* N*) ou* $N = 11, 17, 19, 37, 43, 67$ *ou* 163.

Les valeurs N = 11, 17, 19, . . ., 163 sont des nombres premiers pour lesquels le corps quadratique imaginaire $\mathbb{Q}(\sqrt{-N})$ a un nombre de classes égal à 1. Les courbes elliptiques avec multiplication complexe par les ordres maximaux de ces corps admettent des modèles sur $\mathbb{Q}$ et le noyau de la multiplication par $\sqrt{-N}$ donne un sous-groupe cyclique d'ordre N dans E, défini sur $\mathbb{Q}$. La finesse de l'argument de Mazur se mesure au fait qu'il tient compte de ces exceptions arithmétiquement non triviales tout en excluant toutes les autres occurrences possibles.

Sheldon Kamienny a généralisé le théorème 1, ce qui a conduit à la classification des sous-groupes de torsion possibles pour les courbes elliptiques définies sur des corps de nombres de petit degré sur $\mathbb{Q}$ (voir [130] et [38]). Le résultat le plus abouti dans cette direction a ensuite été obtenu par Loïc Merel [135], qui a montré que les sous-groupes de torsion des courbes elliptiques définies sur un corps de nombres K sont bornés par une constante B_K qui ne dépend que de K, et même seulement du degré de K sur $\mathbb{Q}$.

5 Points rationnels sur les courbes modulaires

Les théorèmes 1 et 2 peuvent être reformulés en termes de points rationnels sur les courbes modulaires, qui apparaissent naturellement comme des espaces de modules paramétrant les classes d'isomorphisme des courbes elliptiques avec des « structures de niveau » auxiliaires.

Si E est une courbe elliptique sur un corps F dans lequel 6 est inversible, il existe deux fonctions rationnelles x et y qui sont régulières sur $E - \{O\}$, qui ont des pôles d'ordre 2 et 3 respectivement en O, et qui satisfont une équation de la forme

$$y^2 = x^3 + ax + b, \quad \text{avec } a, b \in F.$$

Les fonctions x et y sont déterminées de manière unique par ces propriétés au remplacement de (x, y) par $\left(t^2x, t^3y\right)$ pour un certain $t \in F^\times$ près, ce qui a pour effet de remplacer les coefficients (a, b) par $\left(t^4a, t^6b\right)$. En particulier, l'expression

$$j(E) := 1728\frac{4a^3}{4a^3 + 27b^2},$$

appelée j-invariant de E, ne dépend que de (la classe d'isomorphisme $\bar{F}$ de) E et non du choix de x et y. Il s'agit en fait d'un invariant d'isomorphisme complet : deux courbes elliptiques sur F sont isomorphes

(sur la clôture algébrique de F) précisément lorsqu'elles ont le même j-invariant. La j-droite affine, vue comme une courbe algébrique sur $\mathbb{Q}$, est donc un espace de modules (grossier) de courbes elliptiques : ses points sur tout corps F de caractéristique nulle sont en bijection avec les classes d'isomorphisme $\bar{F}$ des courbes elliptiques sur F. Cette j-droite affine est l'exemple le plus simple de courbe modulaire.

On obtient des exemples plus intéressants en classifiant les courbes elliptiques avec une structure de niveau supplémentaire. Une structure typique de niveau N sur E équivaut à la donnée d'un sous-groupe ou d'un point d'ordre N sur E, ou éventuellement à une base pour la N-torsion complète de E. Les courbes qui classent les solutions de ces problèmes sont communément appelées $Y_0(N)$, $Y_1(N)$ et $Y(N)$ respectivement. Ce sont des courbes affines sur $\mathbb{Q}$, qui peuvent être complétées en courbes projectives lisses en leur adjoignant un ensemble fini de *cusps* : les courbes projectives résultantes sont appelées $X_0(N)$, $X_1(N)$ et $X(N)$.

Par exemple, toute courbe elliptique admet une application π de degré 2 dans $\mathbb{P}_1$ qui est ramifiée précisément en l'ensemble E[2] de ses points de 2-torsion. La donnée supplémentaire d'une base (P_1, P_2) pour E[2] sur F peut être utilisée pour rigidifier le choix de π en exigeant que

$$\pi(P_1) = 0, \quad \pi(P_2) = 1, \quad \pi(O) = \infty.$$

L'invariant $\lambda := \pi(P_1 + P_2) \in F - \{0, 1\}$ détermine le triplet (E, P_1, P_2) de manière unique à isomorphisme sur $\bar{F}$ près, et l'application $(E, P_1, P_2) \mapsto \lambda$ donne une identification

$$Y(2) = \mathbb{P}_1 - \{0, 1, \infty\}$$

dans laquelle $\lambda \in \mathbb{P}_1$ correspond à la courbe elliptique de Legendre $y^2 = x(x-1)(x-\lambda)$ de base $((0,0),(0,1))$ pour ses points de 2-division.

Ce qui suit est simplement une reformulation du théorème 2 du point de vue des points rationnels sur les courbes modulaires :

Théorème 3. *Soit* N *un nombre premier pour lequel* $Y_0(N)(\mathbb{Q})$ *est non vide. Alors* $N = 2, 3, 5, 7, 13$ *(lorsque* $X_0(N)$ *est isomorphe à la droite projective et possède une infinité de points rationnels) ou* $N = 11, 17, 19, 37, 43, 67$ *ou* 163 *(lorsque* $Y_0(N)$ *contient un ensemble fini de points rationnels « sporadiques »).*

Il est possible d'écrire des équations concrètes (mais finalement peu utiles) pour les courbes modulaires. Si E et E′ sont liées par une isogénie

cyclique de degré N, alors leurs j-invariants j et j' donnent lieu à une racine (j, j') du polynôme modulaire $\Phi_N(x, y)$, qui est un polynôme rationnel de bidegré N + 1 lorsque N est un nombre premier. La courbe $Y_0(N)$ est birationnellement équivalente à la courbe plane définie par ce polynôme. Ces équations de définition ont tendance à être assez compliquées. Par exemple,

$$\begin{aligned}\Phi_2(x, y) = {} & x^3 - x^2y^2 + 1488\,x^2y - 162\,000\,x^2 + 1488\,xy^2 + 40\,773\,375\,xy \\ & + 8\,748\,000\,000\,x + y^3 - 162\,000\,y^2 + 8\,748\,000\,000\,y \\ & - 157\,464\,000\,000\,000.\end{aligned}$$

S'attaquer aux équations diophantiennes associées par une approche élémentaire directe semble décidément peu prometteur.

La première ruse de Mazur est de plonger la courbe modulaire, disons $X_0(N)$, dans sa jacobienne $J_0(N)$, une variété abélienne dont les points rationnels peuvent alors être étudiés par la méthode de descente infinie de Fermat dans le cadre conceptuel moderne donné par André Weil, dans lequel la considération d'équations explicites peut être largement évitée.

Mazur est capable de montrer que si N est un nombre premier pour lequel $J_0(N)$ n'est pas trivial (c'est-à-dire si N = 11 ou N > 13), alors cette jacobienne admet des quotients non triviaux avec un groupe de Mordell-Weil fini sur $\mathbb{Q}$, qu'il appelle quotients d'Eisenstein. Ceci implique immédiatement, une décennie avant la démonstration par Faltings de la conjecture de Mordell, que $X_0(N)$ a un nombre fini de points rationnels chaque fois qu'il a un genre $\geqslant 1$. Avec plus d'attention, on peut aussi utiliser ceci pour obtenir des bornes sur l'ensemble des points rationnels suffisamment précises pour en déduire le théorème 1 et avec encore plus d'attention le théorème 2.

Les quotients d'Eisenstein de $J_0(N)$ sont associés aux différents nombres premiers p qui divisent le numérateur de $(N - 1)/12$ et sont notés $J_{\mathrm{eis}}^{(p)}(N)$. Le groupe de Mordell-Weil $J_{\mathrm{eis}}^{(p)}(N)(\mathbb{Q})$ contient un élément d'ordre p. Il devient naturel de calculer ce groupe de Mordell-Weil par un argument de p-descente impliquant le groupe de Selmer pour un module de p-torsion sur lequel le groupe de Galois de $\mathbb{Q}$ agit par l'intermédiaire d'un quotient abélien. La « descente d'Eisenstein » que Mazur a développée à cette fin place donc l'étude de $J_{\mathrm{eis}}^{(p)}(\mathbb{Q})$ à proximité de questions plus classiques concernant les groupes de classes des corps cyclotomiques.

En construisant $J_{\mathrm{eis}}^{(p)}$ et en établissant la finitude de son groupe

de Mordell-Weil, Mazur a pu rassembler plusieurs caractéristiques spéciales des courbes modulaires qui rendent leurs propriétés diophantiennes plus faciles à analyser. Plus important encore, les courbes modulaires sont dotées d'un grand nombre de correspondances algébriques sur $\mathbb{Q}$, qui émergent naturellement de la description de leurs modules et sont des incarnations géométriques des opérateurs de Hecke. Les endomorphismes ainsi obtenus décomposent $J_0(N)$ en morceaux arithmétiquement plus simples avec une grande algèbre d'endomorphismes, dont les modules de Tate donnent lieu à des (systèmes compatibles de) représentations bidimensionnelles ℓ-adiques de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Ces quotients de variétés abéliennes « de type **GL**(2) » offrent un terrain d'essai fertile pour le programme général de compréhension des représentations linéaires des groupes de Galois des corps de nombres, pierre angulaire du programme de Langlands. Les représentations bidimensionnelles de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ représentent une première étape typique de ce programme, dépassant le cadre abélien de la théorie globale des corps de classes. C'est en partie pour cette raison que la descente d'Eisenstein de Mazur a largement dépassé en importance l'application diophantienne pour laquelle elle a été conçue à l'origine. Les idées que Mazur a introduites dans le sujet ont joué un rôle clé, notamment dans la démonstration par Andrew Wiles [148] près de vingt ans plus tard de la conjecture de Taniyama-Weil sur la modularité des courbes elliptiques sur $\mathbb{Q}$, comme nous l'expliquerons plus loin.

Le point non trivial d'ordre p sur $J_0(N)$ que Mazur exploite de façon si spectaculaire dans ses démonstrations des théorèmes 1 et 2 provient de l'image d'un diviseur dont le support est sur les *cusps* de $X_0(N)$. En plus des *cusps*, la courbe modulaire $X_0(N)$ est également dotée d'un grand nombre de points définis sur divers corps de classes d'anneaux de corps quadratiques imaginaires, les points de Heegner provenant des modules de courbes elliptiques appropriées avec multiplication complexe. Une formule de Benedict Gross et Don Zagier relie les hauteurs de ces points aux dérivées premières de la fonction L de Hasse-Weil des variétés abéliennes quotients de $J_0(N)$. À la fin des années quatre-vingt, Victor Kolyvagin a transformé ce lien en une démonstration de la finitude du groupe de Mordell-Weil de tout quotient de $J_0(N)$ dont la fonction L de Hasse-Weil ne s'annule pas au centre, en accord avec la conjecture de Birch et Swinnerton-Dyer pour ces quotients. Le quotient un peu plus grand de $J_0(N)$ avec un groupe de Mordell-Weil fini qui émerge du théorème de Kolyvagin est appelé le quotient d'enroulement (une terminologie qui peut être retracée jusqu'à l'« élément d'enroulement »

de Mazur [42]). Le quotient d'enroulement a été exploité plus tard à bon escient par Merel dans sa généralisation du théorème 1 à des corps de nombres de degré arbitraire [135].

6 Le dernier théorème de Fermat

Le théorème 3 de Mazur sur les points rationnels des courbes modulaires affirme qu'une collection infinie de courbes, de genre et de complexité arithmétique croissants, les courbes modulaires $X_0(N)$ indexées par le paramètre N, n'ont pas de points rationnels sauf les points triviaux lorsque N est suffisamment grand. Cet énoncé rappelle le dernier théorème de Fermat, qui fait la même affirmation pour les courbes de Fermat F_N d'équation

$$F_N : x^N + y^N = z^N.$$

La relation entre les deux énoncés va bien au-delà d'une analogie superficielle. Le théorème 3 s'avère être un ingrédient critique, en fait l'ingrédient diophantien clé, dans la démonstration du dernier théorème de Fermat.

Le lien étroit entre les propriétés diophantiennes des courbes modulaires et des courbes de Fermat peut sembler surprenant à première vue, puisqu'il n'existe que rarement des applications explicites entre les deux types de courbes. Une exception charmante à cette affirmation est la courbe modulaire X(7) avec une structure complète de niveau 7, une courbe de genre 3 ayant un groupe d'automorphismes de taille maximale pour son genre, le groupe PSL(2, 7) d'ordre 168 . Cette propriété la détermine de façon unique à isomorphisme sur $\overline{\mathbb{Q}}$ près. Un modèle pour elle est fourni par la célèbre quartique de Klein d'équation

$$X(7) : u^3v + v^3w + w^3u = 0$$

Il s'avère que X(7) est l'image de la courbe de Fermat

$$F_7 : x^7 + y^7 + z^7 = 0$$

par l'application $\pi : F_7 \to X(7)$ de degré 7 qui envoie $(x, y, z) \in F_7$ vers

$$(u, v, w) = \pi(x, y, z) := \left(x^3z, y^3x, z^3y\right)$$

Une solution non triviale du dernier théorème de Fermat donnerait donc lieu à un point rationnel non trivial sur X(7). L'affirmation que

cette courbe modulaire n'a pas de points rationnels non triviaux, c'est-à-dire tels que $uvw \neq 0$, implique donc le dernier théorème de Fermat pour l'exposant 7. Plus intéressante est l'implication inverse qui a été démontrée pour la première fois par Hurwitz, à savoir que X(7) n'a pas de points rationnels non triviaux parce qu'il en est de même pour F_7. À l'époque, le dernier théorème de Fermat pour l'exposant 7 était déjà connu grâce aux travaux de Lamé. Hurwitz note que si (u, v, w) est un point de la quartique de Klein avec des coordonnées entières telles que $\mathrm{pgcd}(u, v, w) = 1$, alors ces coordonnées n'ont pas besoin d'être premières entre elles deux à deux. En posant

$$x = \mathrm{pgcd}(u, v), \quad y = \mathrm{pgcd}(v, w), \quad z = \mathrm{pgcd}(w, u),$$

un raisonnement direct impliquant le théorème fondamental de l'arithmétique montre (après avoir changé les signes de x, y ou z si nécessaire) que (x, y, z) est situé sur la courbe de Fermat F_7 et que $\pi(x, y, z) = (u, v, w)$. Par cet argument, Hurwitz montre que l'application $\pi : F_7 \to X(7)$ est surjective sur les points rationnels. Contrairement à l'implication purement algébrique

$$\begin{aligned} & F_7 \text{ a un point rationnel non trivial} \\ \Rightarrow \quad & X(7) \text{ a un point rationnel non trivial,} \end{aligned} \tag{1}$$

l'implication inverse est plus authentiquement arithmétique et repose sur des ingrédients tels que la factorisation unique. Le fait que l'application π de degré 7 (vue par exemple comme une application des surfaces de Riemann sur les points complexes des courbes) est partout non ramifiée est essentiel pour cette implication.

La démonstration du dernier théorème de Fermat pour l'exposant (premier) p général repose sur une relation géométrique analogue mais substantiellement plus générale entre la courbe modulaire $X(2p)$ et la p-ième courbe de Fermat F_p. En effet, toutes deux sont munies d'applications surjectives naturelles

$$F_p \xrightarrow{\pi_1} \mathbb{P}_1 \xleftarrow{\pi_2} X(2p)$$

sur la droite projective $\mathbb{P}_1$ avec des « caractéristiques locales communes ». L'application π_1 envoie le triplet de Fermat (x, y, z) vers x^p/y^p et l'application π_2 est simplement celle qui « oublie la structure de niveau p », envoyant un point de $X(2p)$ vers son image naturelle dans $X(2)$, identifiée avec la droite projective en considérant $\lambda \in \mathbb{P}_1$ comme

le paramètre dans la famille de Legendre des courbes elliptiques

$$y^2 = x(x-1)(x-\lambda).$$

Bien qu'elles aient des degrés différents et qu'elles soient définies sur des courbes différentes, les applications π_1 et π_2 présentent l'affinité frappante suivante : elles sont toutes deux ramifiées uniquement en 0, 1 et ∞, et leurs degrés de ramification en ces trois points sont égaux à p. Cela suggère que, si $(a,b,c) \in \mathrm{F}_p(\mathbb{Q})$ est une solution non triviale du dernier théorème de Fermat, alors l'image $\pi_1(a,b,c) = a^p/b^p \in \mathbb{P}_1(\mathbb{Q})$ devrait se relever en un point de $\mathrm{X}(2p)$ dont le corps de définition présente une ramification limitée, bornée indépendamment de la solution (a,b,c). On est amené à étudier le corps engendré par les points de p-division de la « courbe elliptique de Frey »

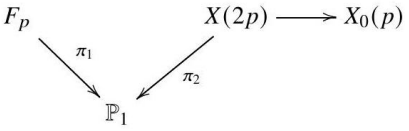
$$\mathrm{E}_{a,b,c} : y^2 = x\,(x-a^p)\,(x+b^p)\,,$$

qui est en effet (après avoir éventuellement réordonné a, b et c de façon appropriée et modifié leurs signes) non ramifiée en dehors de 2 et p.

La démonstration ultime du dernier théorème de Fermat repose sur une analyse extrêmement délicate de ce corps ou mieux encore de la représentation linéaire sur $\mathbb{Z}/p\mathbb{Z}$

$$\varrho_{a,b,c} : \mathrm{G}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(\mathrm{E}_{a,b,c}[p]) \simeq \mathbf{GL}_2(\mathbb{Z}/p\mathbb{Z})$$

du groupe de Galois absolu de $\mathbb{Q}$ agissant sur les points de p-torsion de $\mathrm{E}_{a,b,c}$. L'idée surprenante qui a émergé des travaux de Gerhard Frey, Jean-Pierre Serre [143] et Kenneth Ribet [141] est que la modularité de $\mathrm{E}_{a,b,c}$, qui a finalement été démontrée par Wiles [148], peut être transformée en la conclusion que $\varrho_{a,b,c}$ est nécessairement réductible. De ce fait, toute solution non triviale $(a,b,c) \in \mathrm{F}_p(\mathbb{Q})$ au dernier théorème de Fermat peut être transférée en un point rationnel non trivial sur $\mathrm{X}_0(p)$, en la poursuivant à travers le diagramme suivant d'applications de courbes :



Grâce à l'implication

$$\begin{aligned} & \mathrm{F}_p \text{ a un point rationnel non trivial} \\ \Rightarrow \quad & \mathrm{X}_0(p) \text{ a un point rationnel non trivial,} \end{aligned} \tag{2}$$

(qui rappelle (1), qui est encore plus proche dans l'esprit de sa réciproque et qui est considérablement plus profond que les deux énoncés), une question diophantienne sur les courbes de Fermat F_p se réduit à la même question sur les courbes modulaires $X_0(p)$, précisément la question à laquelle répond le théorème 3 de Mazur.

Comme nous l'expliquerons plus en détail dans la section 10, les idées introduites par Mazur pour démontrer le théorème 3 sont également déterminantes pour la démonstration de (2) : elles sont donc tissées dans la trame même de l'extraordinaire démonstration de Wiles de la conjecture de Taniyama-Weil et du dernier théorème de Fermat.

7 Les conjectures principales d'Iwasawa

Références : [45, 47, 51].

La démonstration de la conjecture principale de la théorie d'Iwasawa par Mazur et Wiles [47] est un autre événement marquant en théorie des nombres qui est survenu environ dix ans avant la démonstration du dernier théorème de Fermat. La théorie d'Iwasawa part du fait que les p-parties des groupes des classes d'idéaux des corps cyclotomiques pour une puissance de p, obtenus en adjoignant à $\mathbb{Q}$ les racines p^n-ièmes de l'unité, présentent une croissance remarquablement régulière en fonction de n. La conjecture principale de la théorie d'Iwasawa lie ce comportement aux zéros de la fonction zêta p-adique de Kubota-Leopoldt. Elle est née d'une analogie avec la formulation par Weil de l'hypothèse de Riemann pour les variétés sur les corps finis, et peut être envisagée comme sa contrepartie dans un cadre p-adique, dans la mesure où elle attribue aux mystérieux zéros de la fonction zêta p-adique une interprétation spectrale. Ces zéros sont les valeurs propres d'un certain opérateur — un générateur topologique du groupe de Galois du prolongement $\mathbb{Z}_p$-cyclotomique engendré par toutes les racines de l'unité pour une puissance de p — agissant sur un module d'Iwasawa formé par l'assemblage des groupes des classes d'idéaux des couches finies de ce $\mathbb{Z}_p$-prolongement. Une caractéristique remarquable de la démonstration de Mazur et Wiles est qu'elle repose sur une étude minutieuse des représentations galoisiennes bidimensionnelles issues des quotients des jacobiennes des courbes modulaires, en particulier celles qui sont réductibles, pour démontrer un énoncé qui fait ostensiblement partie de la théorie abélienne plus classique des groupes de classes des corps cyclotomiques. La théorie globale des corps de classes

est utilisée pour convertir les questions relatives aux groupes de classes en questions relatives à la construction d'extensions abéliennes non ramifiées de corps cyclotomiques, et les extensions qui sont censées découler des zéros de la fonction zêta p-adique se révèlent finalement être coupées par les représentations galoisiennes qui découlent des points de torsion p-primaires de ces jacobiennes modulaires.

La démonstration de la conjecture principale d'Iwasawa, qui justifie l'analogie entre la fonction zêta p-adique de Kubota-Leopoldt et le polynôme d'Alexander d'un nœud que Mazur avait perçue des décennies plus tôt, est l'une des réalisations les plus remarquables de la théorie des nombres dans la seconde moitié du xx^{e} siècle. Sa méthode a été largement généralisée, notamment par Wiles pour les corps totalement réels [147] et par Chris Skinner et Eric Urban [144] dans le cadre des courbes elliptiques, un cadre qui doit également beaucoup à la vision de Mazur et dont il sera question dans la section suivante.

8 Courbes elliptiques et conjecture de Birch et Swinnerton-Dyer

Références : [40, 44, 46, 48, 50, 52, 56, 58, 101].

Tout au long des années soixante-dix et quatre-vingt, Mazur a longuement réfléchi à l'arithmétique des courbes elliptiques, en se concentrant sur le problème ouvert notoirement le plus difficile et le plus central dans ce domaine : la conjecture de Birch et Swinnerton-Dyer. Plutôt que de s'attaquer de front à ce problème, il a lancé une étude parallèle dans le cadre p-adique, ouvrant ainsi un nouveau sujet de recherche qui s'est avéré remarquablement fructueux et qui a vu des décennies de progrès soutenus.

L'article [41] défend l'introduction des idées de la théorie d'Iwasawa dans l'étude arithmétique des courbes elliptiques et des variétés abéliennes. Les modules d'Iwasawa pertinents sont obtenus en remplaçant les p-parties des groupes des classes d'idéaux par les p-groupes de Selmer pertinents sur les couches finies d'une $\mathbb{Z}_p$-extension, convenablement assemblés. L'importance de cette nouvelle perspective peut difficilement être surestimée : des carrières mathématiques entières (dont celle de l'auteur) ont été agréablement passées à développer la vision de Mazur pour la théorie d'Iwasawa des variétés abéliennes sur les tours de corps de nombres.

L'article de Mazur et Peter Swinnerton-Dyer [42] introduit ce qui est maintenant connu comme la fonction L p-adique de Mazur-Swinnerton-

Dyer d'une courbe elliptique sur $\mathbb{Q}$, la contrepartie directe de la fonction L de Hasse-Weil dans le monde p-adique. La relation entre les fonctions L p-adiques définies analytiquement comme celle-ci et les séries caractéristiques des modules d'Iwasawa de Mazur conduit à une riche variété de « conjectures principales d'Iwasawa » pour les courbes elliptiques.

Les bases posées dans [41] et [42] conduisent naturellement à un analogue p-adique de la conjecture de Birch et Swinnerton-Dyer, qui a été formulé environ dix ans plus tard dans un article très influent de Mazur, Tate et Teitelbaum [50].

La conjecture de Birch et Swinnerton-Dyer p-adique est plus facile à traiter que son précurseur archimédien en raison du lien étroit que l'on peut espérer établir entre les fonctions L p-adiques et les modules d'Iwasawa de Mazur, tel qu'exprimé dans la conjecture principale. La conjecture principale explique par exemple pourquoi les courbes elliptiques de rang élevé devraient présenter des zéros d'ordre élevé dans leurs fonctions L p-adiques associées : c'est parce que le groupe de Mordell-Weil fournit un sous-espace du module d'Iwasawa pertinent qui est fixé par Galois et contribue ainsi à la multiplicité du caractère trivial en tant que zéro de la fonction L p-adique.

Une telle interprétation spectrale fait cruellement défaut pour les zéros de la fonction L de Hasse-Weil dans le cadre archimédien. En effet, il n'existe pas une seule courbe elliptique sur $\mathbb{Q}$ dont on puisse montrer que la série L s'annule à l'ordre > 3 en $s = 1$, bien qu'on sache que des courbes elliptiques de rang > 3 (et même > 23) existent en relative abondance.

On comprend mieux la situation dans le cadre non archimédien dont Mazur a été le pionnier. La divisibilité requise dans la conjecture principale pour les courbes elliptiques sur $\mathbb{Q}$ a été démontrée par Kazuya Kato au début des années quatre-vingt-dix en exploitant, un peu comme Kolyvagin avec les points de Heegner, des éléments spéciaux de la K-théorie des courbes modulaires provenant de paires d'unités de Siegel et (de façon cruciale) de leurs déformations p-adiques [131]. Grâce au résultat de Kato, on sait que la fonction L p-adique de Mazur-Swinnerton-Dyer d'une courbe elliptique s'annule à un ordre au moins égal au rang du groupe de Mordell-Weil.

La divisibilité opposée dans la conjecture principale pour les courbes elliptiques a été établie par Skinner et Urban [144], en s'appuyant sur le faisceau d'idées très différent qui est apparu dans la démonstration de la conjecture principale d'Iwasawa originale par Mazur et Wiles. D'importants mystères liés à la finitude du groupe de Chafarevitch-Tate

et à la non-dégénérescence des hauteurs p-adiques (et la non-semi-simplicité éventuelle des modules d'Iwasawa concernés) empêchent encore cette divisibilité dans la conjecture principale de conduire à la majoration correcte sur l'ordre d'annulation de la fonction L p-adique. Ainsi, la conjecture de Birch et Swinnerton-Dyer p-adique de Mazur, Tate et Teitelbaum offre toujours des mystères séduisants malgré son accessibilité relative par rapport à la conjecture archimédienne originale.

Une autre caractéristique intéressante de la conjecture de Birch et Swinnerton-Dyer p-adique est l'apparition de nouveaux phénomènes qui semblent ne pas avoir de contrepartie immédiate dans le cadre archimédien, notamment le phénomène des zéros exceptionnels des fonctions L p-adiques qui peuvent provenir par exemple de l'annulation d'un facteur d'Euler en p qui doit être inséré pour assurer l'interpolation des valeurs spéciales. Ce phénomène a été observé et étudié pour la première fois dans [50]. Bien qu'ils puissent sembler quelque peu spécialisés pour les non-initiés, les termes principaux des fonctions L p-adiques aux points où il y a un zéro exceptionnel recèlent de riches informations arithmétiques. Leur examen attentif est souvent récompensé par de nouvelles perspectives fructueuses. La « conjecture du zéro exceptionnel » de Mazur, Tate et Teitelbaum concernait la période p-adique de Tate d'une courbe elliptique avec réduction multiplicative. Une série de propositions suggestives ont été formulées pour étendre cette conjecture aux formes modulaires de poids plus élevé, notamment par Jeremy Teitelbaum [145] en termes de théorie de Cherednik-Drinfeld de l'uniformisation p-adique des courbes de Shimura, et par Fontaine et Mazur [67] en exploitant le module de monodromie de Frobenius filtré que la théorie de Hodge p-adique associe à la représentation galoisienne locale p-adique d'une forme modulaire de poids plus élevé. Comme autre exemple de l'importance des zéros exceptionnels, mentionnons qu'ils apparaissent parfois dans les séries L p-adiques associées aux caractères totalement impairs des corps totalement réels en $s = 0$, où ils jouent un rôle central dans la variante p-adique de Gross des conjectures de Stark.

Vers la fin des années quatre-vingt, Mazur a également introduit, en collaboration avec John Tate, un raffinement modeste de la conjecture de Birch et Swinnerton-Dyer p-adique, qui consiste en gros à remplacer l'algèbre d'Iwasawa — l'anneau de groupe complété du groupe de Galois d'une $\mathbb{Z}_p$-extension — par l'anneau de groupe du groupe de Galois d'une extension abélienne finie [52]. Les conjectures plus raffinées qui émergent ainsi s'avèrent offrir un cadre propice à l'étude et à

l'organisation du comportement des systèmes d'Euler. Ces idées ont connu un renouveau récent, notamment grâce à leurs liens avec les conjectures de Harris et Venkatesh concernant les « opérateurs de Hecke dérivés » de Venkatesh agissant sur la cohomologie des faisceaux cohérents sur les courbes modulaires attachées à des formes modulaires de poids un [129].

9 La conjecture de Fontaine-Mazur

Comme beaucoup de grands théoriciens des nombres du xx^{e} siècle, Mazur a contribué de manière significative à l'étude des représentations galoisiennes et de leur lien avec les formes automorphes. Ces idées sont au cœur d'un certain nombre de travaux de Mazur qui ont déjà été évoqués.

L'une des contributions importantes de Mazur dans cette direction est la conjecture profonde, formulée dans [71] avec Jean-Marc Fontaine, qui est désormais généralement connue sous le nom de conjecture de Fontaine-Mazur. Elle vise à caractériser les représentations galoisiennes globales p-adiques qui proviennent de la cohomologie étale p-adique des variétés sur les corps de nombres. La caractérisation se fait *via* leur restriction au groupe de décomposition en p — on exige que ces représentations p-adiques des groupes de Galois des corps p-adiques soient *potentiellement semi-stables*, une notion basée sur des foncteurs de comparaison entre la cohomologie étale p-adique sur les corps p-adiques et les cohomologies p-adiques étudiées par Mazur dans les décennies précédentes — combinée avec une exigence naturelle d'être ramifiées en un nombre fini de nombres premiers autres que p. Cette conjecture fournit un cadre élégant dans lequel la plupart des progrès récents du programme de Langlands peuvent être compris et conceptualisés.

10 Déformations des représentations galoisiennes

Références : [53, 54, 61, 73, 75, 76, 78, 108].

La variation p-adique des formes modulaires et des représentations galoisiennes est un thème qui sous-tend une grande partie du travail de Mazur en théorie des nombres, en commençant par ses premiers travaux sur l'idéal d'Eisenstein. Son article fondamental [53] formalise cette notion du côté de la théorie galoisienne en introduisant

l'anneau de déformation universelle associé à une représentation galoisienne avec des coefficients dans un anneau local complet. Avec cette idée, Mazur a lancé le nouveau domaine de la théorie des déformations galoisiennes, qui a trouvé une application spectaculaire presque immédiatement après sa création dans la démonstration par Wiles de la conjecture de Taniyama-Weil. Cette démonstration procède par la construction d'une application naturelle d'un des anneaux de déformation galoisienne universelle de Mazur vers un anneau convenablement complété d'opérateurs de Hecke, et en montrant que cette application est un isomorphisme. L'étude approfondie de la structure théorique des algèbres de Hecke complétées avait déjà été initiée plus d'une décennie auparavant dans les travaux de Mazur sur l'idéal d'Eisenstein. Avec l'introduction des anneaux de déformation universelle, Mazur peut être crédité d'une partie substantielle de l'infrastructure théorique qui a permis la démonstration de la conjecture de Taniyama-Weil. Les idées de Mazur sont donc présentes dans les fondements mêmes de la stratégie remarquablement réussie pour établir la modularité des représentations galoisiennes qui a été largement développée et généralisée dans le sillage de la percée de Wiles sur la modularité des courbes elliptiques.

Les travaux ultérieurs de Mazur [73,78] avec Robert Coleman représentent une tentative de globaliser partiellement l'étude des espaces de déformation des représentations galoisiennes, conduisant à la notion fondamentale de « courbes propres » et de « variétés propres » de Coleman-Mazur. Le cadre initié par Coleman et Mazur dans ces articles fondateurs a été largement développé au cours des dernières décennies, donnant naissance à un domaine fructueux qui sous-tend une grande partie des progrès récents du programme de Langlands par le biais de méthodes p-adiques.

11 Géométrie diophantienne

Références : [49,62,68,70,72,79,86,95,100].

Les travaux de Mazur sur la géométrie diophantienne se distinguent par des idées souvent étonnantes par leur audace. L'article [62] pose la conjecture frappante que si les points rationnels d'une variété V sont denses pour la topologie de Zariski, alors leur adhérence dans $V(\mathbb{R})$ pour la topologie réelle est une union de composantes connexes de $V(\mathbb{R})$.

Les célèbres conjectures formulées par Mazur avec Lucia Caporaso et Joe Harris [70,72], qui affirment que le nombre de points rationnels sur une courbe de genre g sur un corps de nombres K est borné par une fonction de g et de K, et même seulement de g si l'on tolère un nombre fini d'exceptions, sont d'une portée tout aussi grande. [70] montre que cette conjecture, qui est à la fois remarquablement forte et agréablement concrète, découle de la conjecture antérieure de Lang, à l'époque plus largement acceptée, selon laquelle l'ensemble des points rationnels sur une variété de type général ne peut jamais être dense au sens de Zariski.

De telles conjectures intrépides, qui s'appliquent à toutes les variétés à la fois ou au nombre de points sur toutes les courbes d'un genre donné, jettent une lumière inattendue sur de vénérables questions concernant les points rationnels et ont guidé de nombreux efforts ultérieurs de la part d'autres chercheurs.

De nombreux articles de Mazur consacrés à des sujets diophantiens révèlent des liens inattendus avec d'autres thèmes mathématiques. C'est le cas notamment de [109, 114], qui étudient la variation des rangs de 2-Selmer des courbes elliptiques sur les corps de nombres, révélant un lien surprenant entre la notion de « stabilité diophantienne » et le dixième problème de Hilbert sur l'indécidabilité des questions diophantiennes sur certains corps de nombres.

12 Systèmes d'Euler et domaines connexes

Références : [92, 99, 104, 106, 110, 115, 117–120].

La méthode des systèmes d'Euler est une technique puissante qui a émergé à la fin des années quatre-vingt grâce aux travaux de mathématiciens tels que Francisco Thaine, Karl Rubin, Victor Kolyvagin et Kazuya Kato. Elle permet de transformer la présence d'éléments spéciaux dans la cohomologie galoisienne globale (d'un système compatible de représentations galoisiennes p-adiques) en une démonstration d'au moins une inégalité dans la conjecture principale associée. L'existence des éléments globaux composant un système d'Euler est encore mal comprise et leur construction reste autant un art qu'une science.

Les articles [92, 99, 104, 110, 119, 120], tous en collaboration avec Karl Rubin, font partie d'une tentative systématique de formaliser (*via* la notion de ce que les auteurs appellent un « système de Kolyvagin ») la procédure par laquelle de telles collections de classes globales compatibles avec la norme ayant des liens avec le comportement des fonctions

L peuvent être exploitées pour obtenir des résultats allant dans le sens d'une conjecture principale, ou éventuellement d'une contrepartie apprivoisée dans l'esprit de [52]. Les perspectives introduites par Mazur et Rubin ont eu une influence décisive sur toute une génération de chercheurs qui explorent actuellement les ramifications de la méthode des systèmes d'Euler.

13 Vulgarisation

Références : [59, 63, 75, 83, 87, 89, 93, 97, 105, 107, 112, 113, 116, 121, 124, 126].

Mazur est un maître qui se délecte du plaisir lié aux idées mathématiques et philosophiques. Il est l'auteur d'un ensemble fascinant et éclectique d'essais dans lesquels son érudition et sa curiosité intellectuelle vont très loin. Certains de ces essais sont consacrés à de vastes sujets mathématiques tels que le principe local-global en théorie des nombres [63], la théorie des déformations des représentations galoisiennes [75], les questions diophantiennes liées aux puissances parfaites [83], l'idée générale de déformation dans diverses parties des mathématiques [93], la notion de motif [97], la conjecture de Sato-Tate [105] et l'hypothèse de Riemann [121]. D'autres examinent les idées sous l'angle de leur développement historique, en traitant des nombres complexes tels qu'ils étaient envisagés au XVI^{e} siècle [87] ou de l'article fondateur de Hermann Weyl sur la théorie spectrale [112]. Mazur s'est également aventuré dans des sujets plus philosophiques comme les rêves en mathématiques racontés à travers une évocation du « rêve de jeunesse de Kronecker » (*Kronecker Jugendtraum*) [113], le concept de nombre et d'abstraction mathématique [89], le concept subtil et insaisissable d'égalité en mathématiques [107], la notion de plausibilité [116], l'unité globale des mathématiques [124] et des réflexions sur la pratique des mathématiques pendant la pandémie [126]. L'enthousiasme contagieux de Mazur se transmet facilement au lecteur. Ses réflexions sur un large éventail de sujets mathématiques, historiques et philosophiques ne manquent jamais d'enchanter, d'élever l'esprit et d'éclairer. L'étendue et la profondeur des centres d'intérêt de Mazur sont évoquées de manière frappante dans le film documentaire « Barry Mazur et le fromage infini de la connaissance » (*Barry Mazur and the Infinite Cheese of Knowledge*) réalisé par Oliver Ralfe [140].

14 Un mentor

Selon un site de généalogie mathématique, Mazur a eu (au moins) 57 étudiants et 325 descendants, des chiffres qui seront certainement obsolètes au moment où cet éloge sera mis sous presse. Au-delà de l'impact direct qu'il a eu sur ses étudiants, Mazur a façonné les perspectives de toute une génération de théoriciens des nombres qui ont été enrichis par ses idées et ont eu le privilège de poursuivre son vaste héritage intellectuel. Cet héritage, qui est maintenant reconnu par l'attribution de la médaille Chern, est une partie centrale et intégrante de la théorie moderne des nombres. Son influence se fera sentir pendant très longtemps.

Bibliographie

[1] *Publ. math. IHÉS*, nº 3, 1959, p. 5-17.

[2] *Publ. math. IHÉS*, nº 3, 1959, p. 19-27.

[3] *Publ. math. IHÉS*, nº 3, 1959, p. 29-48.

[4] Mazur (Barry), *On Embeddings of Spheres*, thèse, université de Princeton, 1959.

[5] *Bull. Am. Math. Soc.*, nº 65, 1959, p. 59-65.

[6] *Acta Math.*, nº 105, 1961, p. 1-17.

[7] *Ann. Math.*, nº 73, 1961, p. 221-228.

[8] *Bull. Am. Math. Soc.*, nº 67, 1961, p. 377-384.

[9] *Bull. Am. Math. Soc.*, nº 68, 1962, p. 87-92.

[10] *Illinois J. Math.*, nº 6, 1962, p. 245-250.

[11] *Ann. Math.*, nº 77, 1963, p. 232-249.

[12] *Publ. math. IHÉS*, nº 15, 1963, p. 5-93.

[13] *Ann. Math.*, nº 80, 1964, p. 201-226.

[14] *Trans. Am. Math. Soc.*, nº 111, 1964, p. 288-316.

[15] *Ann. Math.*, nº 81, 1965, p. 82-99.

[16] *Differential and Combinatorial Topology*, Princeton University Press, 1965, p. 145-165.

[17] *Topology*, nº 5, 1966, p. 179-189.

[18] *Ann. Math.*, nº 83, 1966, p. 387-401.

[19] Hirsch (Morris W.) et Mazur (Barry), *Smoothings of Piecewise Linear Manifolds*, Princeton University Press, 1974.

[20] *Bull. Am. Math. Soc.*, nº 78, 1972, p. 653-667.

[21] *Ann. Math.*, nº 98, 1973, p. 58-95.

[22] Mazur (Barry) et Messing (William), *Universal Extensions and One Dimensional Crystalline Cohomology*, Springer, 1974.

[23] *Algebraic Geometry*, American Mathematical Society, 1975, p. 231-261.

[24] *Ann. sci. Éc. norm. sup.*, nº 10, 1977, p. 87-131.

[25] *Proceedings of a Conference on Local Fields*, Springer, 1967, p. 1-15.

[26] *Invent. math.* nº 9, 1970, p. 201-234.

[27] *Applications of Categorical Algebra*, American Mathematical Society, 1970, p. 219-225.

[28] Artin (Michael) et Mazur (Barry), *Etale Homotopy*, Springer, 1969.

[29] *Am. J. Math.*, nº 92, 1970, p. 343-361.

[30] `people.math.harvard.edu/ mazur/papers/alexander_polynomial.pdf`.

[31] *Ann. sci. Éc. norm. sup.*, nº 6, 1973, p. 521-552.

[32] *C. r. Acad. sci. A-B*, nº 275, 1972, p. A743-A745.

[33] *Invent. math.*, nº 22, 1973, p. 41-49.

[34] *Séminaire Bourbaki*, nº 17, 1976, exposé nº 469.

[35] *Modular Functions of One Variable V*, Springer, 1977, p. 107-148.

[36] *Publ. math. IHÉS*, nº 47, 1977, p. 33-186.

[37] *Invent. math.*, nº 44, 1978, p. 129-162.

[38] *Astérisque*, nº 228, 1995, p. 81-100.

[39] Katz (Nicholas M.) et Mazur (Barry), *Arithmetic Moduli of Elliptic Curves*, Princeton University Press, 1985.

[40] *Séminaire Bourbaki*, nº 14, 1973, exposé nº 414.

[41] *Invent. math.*, nº 18, 1972, p. 183-266.

[42] *Invent. math.*, nº 25, 1974, p. 1-61.

[43] *Proceedings of the International Congress of Mathematicians (Vancouver, 1974)*, vol. I, p. 369-377.

[44] *Invent. math.*, nº 55, 1979, p. 207-240.

[45] *Am. J. Math.*, nº 105, 1983, p. 507-521.

[46] *Arithmetic and Geometry*, Boston, Birkhäuser, 1983, vol. I, p. 195-237.

[47] *Invent. math.*, nº 76, 1984, p. 179-330.

[48] *Proceedings of the International Congress of Mathematicians*, Varsovie, PWN, 1984, vol. I-II, p. 185-211.

[49] *Bull. Am. Math. Soc.*, nº 14, 1986, p. 207-259.

[50] *Invent. math.*, nº 84, 1986, p. 1-48.

[51] *Compositio Math.*, nº 59, 1986, p. 231-264.

[52] *Duke Math. J.*, nº 54, 1987, p. 711-750.

[53] *Galois Groups over Q*, Springer, 1989, p. 385-437.

[54] *Algebraic Number Theory*, Academic Press, 1989, p. 1-21.

[55] *Compositio Math.*, nº 74, 1990, p. 115-133.

[56] *Publ. math. IHÉS*, nº 71, 1990, p. 65-103.

[57] *J. Am. Math. Soc.*, nº 4, 1991, p. 1-23.

[58] *Duke Math. J.*, nº 62, 1991, p. 663-688.

[59] *Am. Math. Mon.*, nº 98, 1991, p. 593-610.

[60] *Astérisque*, nº 196-197, 1991, p. 215-255.

[61] *Math. Comput.*, nº 58, 1992, p. 793-805.

[62] *Exp. Math.*, nº 1, 1992, p. 35-45.

[63] *Bull. Am. Math. Soc.*, nº 29, 1993, p. 14-50.

[64] *Ann. Inst. Fourier*, nº 43, 1993, p. 301-312.

[65] Friedlander (Eric M.) et Mazur (Barry), *Filtrations on the Homology of Algebraic Varieties*, American Mathematical Society, 1994.

[66] *J. Symbolic Logic*, nº 59, 1994, p. 353-371.

[67] *p-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture*, American Mathematical Society, 1994, p. 1-20.

[68] *Astérisque*, nº 228, 1995, p. 165-182.

[69] *Math. Res. Lett.*, nº 2, 1995, p. 515-536.

[70] *The moduli space of curves*, Birkhäuser, 1995, p. 13-31.

[71] *Elliptic Curves, Modular Forms, & Fermat's Last Theorem*, Cambridge (MA), International Press, 1995, p. 41-78.

[72] *J. Am. Math. Soc.*, nº 10, 1997, p. 1-35.

[73] *Collect. Math.*, nº 48, 1997, p. 151-193.

[74] *J. Reine Angew. Math.*, nº 488, 1997, p. 189-201.

[75] *Modular Forms and Fermat's Last Theorem*, Springer, 1997, p. 243-311,

[76] *Computational Perspectives on Number Theory*, American Mathematical Society, 1998, p. 127-142.

[77] *Duke Math. J.*, nº 95, 1998, p. 125-160.

[78] *Galois Representations in Arithmetic Algebraic Geometry*, Cambridge University Press, 1998, p. 1-113.

[79] *Galois Representations in Arithmetic Algebraic Geometry*, Cambridge University Press, 1998, p. 239-265.

[80] *Current Developments in Mathematics, 1997*, Boston, International Press, 1999, p. 199-203.

[81] *Asian J. Math.*, nº 3, 1999, p. 221-232.

[82] *J. Reine Angew. Math.*, nº 519, 2000, p. 97-141.

[83] *Not. Am. Math. Soc.*, nº 47, 2000, p. 195-202.

[84] *Mathematics : Frontiers and Perspectives*, American Mathematical Society, 2000, p. 433–459.

[85] *Exp. Math.*, nº 9, 2000, p. 13–28.

[86] *Model Theory, Algebra, and Geometry*, Cambridge University Press, 2000, p. 199–227.

[87] *Math. Intell.*, nº 24, 2002, p. 12–21.

[88] *Proceedings of the International Congress of Mathematicians*, Pékin, World Scientific, 2002, vol. II, p. 185–195.

[89] Mazur (Barry), *Imagining numbers (Particularly the Square Root of Minus Fifteen)*, Farrar Straus Giroux, New York, 2003.

[90] *Doc. Math.*, Extra Volume Kato, 2003, p. 585-607.

[91] *Arithmetic of Higher-dimensional Algebraic Varieties*, Birkhäuser, 2004, p. 141–147.

[92] Mazur (Barry) et Rubin (Karl), *Kolyvagin Systems*, American Mathematical Society, 2004.

[93] *Bull. Am. Math. Soc.*, nº 41, 2004, p. 307–336.

[94] *Modular Curves and Abelian Varieties*, Birkhäuser, 2004, p. 151–163.

[95] *The Legacy of Niels Henrik Abel*, Springer, 2004, p. 531–542.

[96] *Stark's Conjectures : Recent Work and New Directions*, American Mathematical Society, 2004, p. 207–221.

[97] *Not. Am. Math. Soc.*, nº 51, 2004, p. 1214–1216.

[98] *Adv. Math.*, nº 198, 2005, p. 504–546.

[99] *J. Differ. Geom.*, nº 70, 2005, p. 1–22.

[100] *Ann. sci. Éc. norm. sup.*, nº 38, 2005, p. 671–692.

[101] *Doc. Math.*, Extra Volume Coates, 2006, p. 577–614.

[102] *Bull. Am. Math. Soc.*, nº 44, 2007, p. 233–254.

[103] *J. Algebra*, nº 314, 2007, p. 419–438.

[104] *Ann. Math.*, nº 166, 2007, p. 579–612.

[105] *Bull. Am. Math. Soc.*, nº 45, 2008, p. 185–228.

[106] *Duke Math. J.*, nº 143, 2008, p. 437–461.

[107] *Proof and Other Dilemmas*, Mathematical Association of America, 2008, p. 221–241.

[108] *J. Inst. Math. Jussieu*, nº 8, 2009, p. 99–177.

[109] *Invent. math.*, nº 181, 2010, p. 541–575.

[110] *Compos. Math.*, nº 147, 2011, p. 56–74.

[111] *Bull. Am. Math. Soc.*, nº 48, 2011, p. 155–209.

[112] *Bull. Am. Math. Soc.*, nº 49, 2012, p. 325–326.

[113] *Circles Disturbed*, Princeton University Press, 2012, p. 183–210.

[114] *Ann. Math.*, nº 178, 2013, p. 287–320.

[115] *Invent. math.*, nº 193, 2013, p. 697–749.

[116] *Math. Intell.*, nº 36, 2014, p. 24–33.

[117] *Compos. Math.*, nº 150, 2014, p. 1077–1106.

[118] *Trans. Am. Math. Soc.*, nº 367, 2015, p. 401–421.

[119] *J. théor. nr. Bordx*, nº 28, 2016, p. 145–183.

[120] *J. théor. nr. Bordx*, nº 28, 2016, p. 185–211.

[121] Mazur (Barry) et Stein (William), *Prime Numbers and the Riemann Hypothesis*, Cambridge University Press, 2016.

[122] *Number Theory Related to Modular Curves*, American Mathematical Society, 2018, p. 81–104.

[123] *Am. J. Math.*, nº 140, 2018, p. 571–616.

[124] *Not. ICCM*, nº 7, 2019, p. 76.

[125] *Proc. Am. Math. Soc. B*, nº 7, 2020, p. 159–169.

[126] *Math. Intell.*, nº 42-4, 2020, p. 1–6.

[127] *Ann. Math.*, nº 189, 2019, p. 885–944.

[128] *Ann. Inst. Fourier*, nº 63, 2013, p. 957–984.
[129] *Exp. Math.*, nº 28, 2019, p. 342–361.
[130] *Invent. math.*, nº 109, 1992, p. 221–229.
[131] *Astérisque*, nº 295, 2004, p. 117–290.
[132] *Astérisque*, nº 63, 1979, p. 113–163.
[133] *J. Nigerian Math. Soc.*, nº 2, 1983, p. 1–16.
[134] *Nagoya Math. J.*, nº 109, 1988, p. 125–149.
[135] *Invent. math.*, nº 124, 1996, p. 437–449.
[136] *Compos. Math.*, nº 52, 1984, p. 115–137.
[137] *J. Fac. Sci. U. Tokyo 1*, nº 33, 1986, p. 441–466.
[138] Morishita (Masanori), *Knots and Primes*, Springer, 2012.
[139] *Invent. math.*, nº 12, 1971, p. 105–111.
[140] Ralfe (Oliver), *Barry Mazur and the Infinite Cheese of Knowledge*, Sheepstreet films.
[141] *Invent. math.*, nº 100, 1990, p. 431–476.
[142] *Math. Intell.*, nº 18, 1996, p. 57–69.
[143] *Duke Math. J.*, nº 54, 1987, p. 179–230.
[144] *Invent. math.*, nº 195, 2014, p. 1–277.
[145] *Invent. math.*, nº 101, 1990, p. 395–410.
[146] `www.youtube.com/watch?v=jvoYgNYKyk0`
[147] *Ann. Math.*, nº 131, 1990, p. 493–540.
[148] *Ann. Math.*, nº 141, 1995, p. 443–551.

Les travaux d'Elliott Lieb (par Rupert L. Frank)

À l'occasion de l'attribution du prix Gauss 2022 à Elliott Lieb, nous donnons un aperçu non technique de certains de ses travaux fondamentaux en physique mathématique. Nous mettons l'accent en particulier sur ses travaux sur les systèmes coulombiens à plusieurs corps et sur les inégalités fonctionnelles.

Elliott Lieb reçoit le prix Gauss 2022

> « pour des contributions mathématiques profondes d'une ampleur exceptionnelle qui ont façonné les domaines de la mécanique quantique, de la physique statistique, de la chimie numérique et de la théorie de l'information quantique. »

J'ai le grand plaisir de féliciter Elliott pour cet honneur. Dans les pages qui suivent, j'essaierai de donner un aperçu non technique de certains de ses travaux fondamentaux.

Lieb est un spécialiste de physique mathématique. Il s'agit d'un domaine qui se situe à la frontière entre la physique et les mathématiques, que Freeman Dyson [*D'Éros à Gaïa*, p. 198] a décrit ainsi :

> « La physique mathématique est une discipline qui s'efforce de comprendre en profondeur les phénomènes physiques en se conformant aux méthodes et au style rigoureux des mathématiques pures. »

Comme le mentionne la citation, Lieb a apporté des contributions révolutionnaires à la fois aux mathématiques et à la physique. À cet égard, il convient de mentionner qu'il y a environ six mois, Lieb s'est vu décerner la médaille de la Société américaine de physique pour des contributions exceptionnelles à la recherche, la plus haute distinction de cette société savante.

L'un des traits distinctifs de l'œuvre de Lieb est son intemporalité. Indépendamment des modes et des tendances, il a travaillé et continue de travailler sur des problèmes qu'il considère comme profonds et fondamentaux. Ce n'est parfois que des décennies plus tard que l'on

Frank (Rupert L.), « The work of Elliott Lieb », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 142-158. DOI 10.4171/ICM2022/216

comprend tout le potentiel de ses idées. Les bornes de Lieb-Robinson démontrées en 1972 et la sous-additivité forte de l'entropie démontrée en 1973 en sont de parfaits exemples. Elles ont toutes deux joué un rôle clé dans la théorie de l'information quantique au XXI^{e} siècle.

La liste des publications de Lieb contient à l'heure où nous écrivons ces lignes 404 articles, le premier datant de 1955 et le plus récent étant sur le point de paraître. Quatre volumes d'« Œuvres choisies » (*Selecta*) ont été publiés à ce jour [26–29]. À l'occasion de son 90^{e} anniversaire, un recueil d'articles de plus de 1 300 pages a été édité [8], dans lequel les contributeurs expliquent le contenu et les ramifications de l'œuvre de Lieb.

Il est impossible de donner une vue d'ensemble de cette œuvre monumentale. J'ai choisi ici deux domaines principaux des recherches de Lieb, à savoir les systèmes quantiques coulombiens à plusieurs corps et les inégalités fonctionnelles. J'ai omis tous les autres, à l'exception d'une brève mention de certains d'entre eux dans la dernière section. Cette sélection est influencée par mes préférences et mon ignorance. Je demande l'indulgence des lecteurs pour toutes les omissions.

1 Les systèmes quantiques coulombiens

L'un des thèmes récurrents des recherches de Lieb depuis le début des années soixante-dix est l'analyse des systèmes quantiques continus à plusieurs corps et en particulier des systèmes de particules qui interagissent par l'intermédiaire des forces coulombiennes. On néglige ici les autres forces, mais cette description convient à la matière ordinaire et à une grande partie du monde de la vie quotidienne. Pour un compte rendu très lisible du programme de recherche de Lieb dans ce domaine, nous recommandons sa conférence Gibbs en 1989 [25], qui contient une description beaucoup plus détaillée que celle que nous fournissons ici.

Nous considérons un système composé de N électrons quantiques et de K noyaux classiques dans $\mathbb{R}^3$. Ces derniers sont fixés aux positions $R_1, \dots, R_K \in \mathbb{R}^3$ et ont des charges $Z_1, \dots, Z_K \in]0, +\infty[$ (en unités où la charge de l'électron est -1). Les propriétés de ce système sont décrites par le hamiltonien

$$H := \sum_{n=1}^{N} (-\Delta_n) - \sum_{n=1}^{N} \sum_{k=1}^{K} \frac{Z_k}{|x_n - R_k|} + \sum_{1 \leqslant n < m \leqslant N} \frac{1}{|x_n - x_m|} + \sum_{1 \leqslant k < \ell \leqslant K} \frac{Z_k Z_\ell}{|R_k - R_\ell|}, \tag{1}$$

qui opère sur les fonctions dans $\mathbb{R}^{3N}$. Nous utilisons ici les coordonnées $x = (x_1, \dots, x_N) \in \mathbb{R}^{3N}$. Les quatre sommes dans la définition du hamiltonien H correspondent respectivement à l'énergie cinétique des électrons, à l'attraction électron-noyau, à la répulsion électron-électron et à la répulsion noyau-noyau.

Ce hamiltonien peut être vu comme un opérateur autoadjoint non borné dans l'espace de Hilbert constitué de toutes les fonctions antisymétriques dans $L^2(\mathbb{R}^{3N})$, c'est-à-dire des fonctions de carré intégrable ψ qui vérifient $\psi(\dots, x_n, \dots, x_m, \dots) = -\psi(\dots, x_m, \dots, x_n, \dots)$ pour tout $n \neq m$. L'antisymétrie reflète le principe d'exclusion de Pauli. On devrait également tenir compte du spin de l'électron, mais cela ne conduit mathématiquement qu'à des changements mineurs. Nous l'ignorerons dans ce qui suit.

L'énergie de l'état fondamental est par définition

$$\inf \operatorname{spec} H\,.$$

C'est la borne inférieure de $\langle \psi, H\psi \rangle$ pour tous les ψ normalisés et antisymétriques.

La caractéristique fondamentale du problème de l'analyse de l'énergie de l'état fondamental de H (et des systèmes quantiques à plusieurs corps en général) est le nombre énorme de dimensions de l'espace de Hilbert sous-jacent. Cela rend un calcul numérique pratiquement impossible. Pour obtenir des résultats quantitatifs, il faut généralement s'appuyer sur des approximations qui sont numériquement plus faciles à traiter. Cette situation souligne l'importance des études analytiques sur le problème de Schrödinger complet et sur sa relation avec les approximations. Lieb a apporté des contributions fondamentales à ce problème, comme nous le verrons dans la suite de cette section.

1.1 La stabilité de la matière

Le problème de la stabilité de la matière consiste à montrer que pour tout $z > 0$, il existe une constante C telle que pour tout $N, K \in \mathbb{N}$, tout $R_1, \dots, R_K \in \mathbb{R}^3$ et tout $Z_1, \dots, Z_K \in [0, z]$,

$$\inf \operatorname{spec} H \geqslant -C\,(N + K)\,. \tag{2}$$

Cette inégalité indique que, bien que le nombre d'interactions croisse *quadratiquement* avec le nombre total de particules, l'énergie de l'état fondamental ne varie que *linéairement*. Ceci est fondamental pour l'existence de la matière telle que nous la connaissons.

Nous insistons sur le fait que la stabilité de la matière dépend de ce que les électrons sont des fermions, c'est-à-dire du fait que H n'est considéré que sur le sous-espace des fonctions antisymétriques dans $L^2(\mathbb{R}^{3N})$ et non sur l'espace entier $L^2(\mathbb{R}^{3N})$. Elle serait fausse sur ce dernier espace plus grand, comme nous le verrons.

La première démonstration de la stabilité de la matière est due à Dyson et Lenard en 1967. Lieb et Thirring en ont donné une nouvelle démonstration en 1975 [44]. Cette dernière démonstration donne une valeur beaucoup plus réaliste pour la constante C dans l'inégalité (2), à savoir environ $C \approx 5$ au lieu du $C \approx 10^{14}$ de Dyson et Lenard. Cela permet également de clarifier la raison de la validité de la stabilité de la matière à un niveau conceptuel. Voici ce que Dyson écrit dans la préface des « Œuvres choisies » d'Elliott Lieb [29] :

> « Notre démonstration était si compliquée et si peu parlante qu'elle a incité Lieb et Thirring à trouver la première démonstration décente [...]. Pourquoi notre démonstration était-elle si mauvaise et pourquoi la leur était-elle si bonne ? La raison est simple. Lenard et moi avons commencé par des astuces mathématiques et nous sommes frayés un chemin à travers une forêt d'inégalités sans aucune compréhension physique. Lieb et Thirring ont commencé par comprendre la physique et ont ensuite trouvé le langage mathématique approprié pour rendre leur compréhension rigoureuse. Notre démonstration était une impasse. La leur était une porte d'entrée dans le nouveau monde des idées [...]. »

Le mécanisme fondamental de la démonstration par Lieb et Thirring de la stabilité de la matière est le fait que les atomes ne forment pas de liaison dans un modèle approximatif de système coulombien connu sous le nom de modèle de Thomas-Fermi (ici, l'absence de liaison signifie mathématiquement que l'énergie de l'état fondamental d'une molécule est simplement la somme des énergies des atomes individuels). L'objectif de Lieb et Thirring était donc de montrer que cette théorie approximative fournit, après un ajustement approprié des constantes, un minorant rigoureux pour l'énergie de l'état fondamental de Schrödinger. Plus loin dans cette section, nous discuterons à la fois du modèle de Thomas-Fermi et d'une inégalité fonctionnelle (connue sous le nom d'inégalité de Lieb-Thirring) qui conduit au minorant annoncé.

Les travaux cités ci-dessus de Lieb et Thirring qui datent de 1975 ont été le point de départ de l'étude approfondie par Lieb du problème de la

stabilité de la matière, un sujet sur lequel il reviendra à plusieurs reprises pendant plusieurs décennies et avec de nombreux collaborateurs. On remarquera entre autres une démonstration de la stabilité de la matière en présence de champs magnétiques qui couvre la valeur physique de la constante de structure fine [33]. Une introduction à ce domaine se trouve dans son livre avec Seiringer intitulé « La stabilité de la matière en mécanique quantique » (*The Stability of Matter in Quantum Mechanics*) [37].

1.2 L'existence de la limite thermodynamique pour la matière réelle avec des forces coulombiennes

Le premier résultat de Lieb sur les systèmes coulombiens à plusieurs corps, avant même ses travaux sur la stabilité de la matière, a résolu un problème ouvert dans les fondements de la physique statistique. En 1969, Lebowitz et lui ont démontré l'existence de la limite thermodynamique pour la matière réelle avec des forces coulombiennes [30].

On considère ici un grand nombre de particules (des électrons et des noyaux par exemple) confinées dans un ouvert Ω de $\mathbb{R}^3$. On considère la limite où Ω tend vers $\mathbb{R}^3$ (dans un sens à préciser) et où les densités des différentes particules (c'est-à-dire le nombre de particules divisé par le volume de Ω) tendent vers des constantes données. Les particules interagissent par l'intermédiaire des forces coulombiennes, comme dans l'équation (1). De plus, on discute généralement de cette question à une température strictement positive donnée. Le théorème de Lieb et Lebowitz stipule que la limite de l'énergie libre correspondante existe, qu'elle est indépendante de la forme des domaines approximatifs Ω, et qu'elle possède les propriétés de convexité et de concavité appropriées.

Le théorème de Lieb et Lebowitz utilise le théorème de stabilité de la matière comme ingrédient. Dans la démonstration de l'existence de la limite thermodynamique, la principale préoccupation est la lente décroissance de $|x|^{-1}$ lorsque $|x| \to \infty$. En effet, l'existence de la limite thermodynamique était connue dans le cas des interactions à courte portée. Dans le cas des interactions à longue portée, la neutralité de la charge est une donnée essentielle. Lieb et Lebowitz exploitent l'écrantage électrostatique de manière très originale *via* le théorème de Newton. Ils sont ainsi amenés à résoudre le problème géométrique de recouvrir efficacement de grosses boules avec des boules plus petites, ce qu'ils résolvent par leur « théorème du fromage ».

1.3 Le modèle de Thomas-Fermi et la théorie de la fonctionnelle de la densité

Dans notre discussion sur la démonstration de la stabilité de la matière par Lieb et Thirring, nous avons déjà mentionné le modèle de Thomas-Fermi d'un système coulombien. Ce modèle a été proposé indépendamment par Thomas et Fermi en 1927, peu de temps après que Schrödinger eut présenté sa théorie. Dans l'approche variationnelle du modèle de Thomas-Fermi, on part de la fonctionnelle d'énergie définie pour toute fonction ρ positive ou nulle sur $\mathbb{R}^3$ par

$$\mathcal{E}[\rho] = \gamma^{\mathrm{TF}} \int_{\mathbb{R}^3} \rho(x)^{\frac{5}{3}}\, dx - \sum_{k=1}^{\mathrm{K}} \int_{\mathbb{R}^3} \frac{\mathrm{Z}_k\, \rho(x)}{|x - \mathrm{R}_k|}\, dx + \mathrm{D}[\rho] + \sum_{1 \leqslant k < \ell \leqslant \mathrm{K}} \frac{\mathrm{Z}_k \mathrm{Z}_\ell}{|\mathrm{R}_k - \mathrm{R}_\ell|}$$

avec

$$\mathrm{D}[\rho] := \frac{1}{2} \iint_{\mathbb{R}^3 \times \mathbb{R}^3} \frac{\rho(x)\, \rho(y)}{|x - y|}\, dx\, dy\,.$$

La fonction ρ décrit la distribution des électrons et son intégrale représente le nombre total d'électrons. Les quatre termes de la définition de $\mathcal{E}$ correspondent respectivement à l'énergie cinétique des électrons, à l'attraction électron-noyau, à la répulsion électron-électron et à la répulsion noyau-noyau. Dans la prochaine sous-section, nous décrirons brièvement comment on peut arriver à l'approximation $\rho^{\frac{5}{3}}$ de l'énergie cinétique. Cette approximation conduit également à une certaine valeur pour la constante $\gamma^{\mathrm{TF}} > 0$.

L'énergie de l'état fondamental dans le modèle de Thomas-Fermi est

$$\inf \left\{ \mathcal{E}[\rho] :\ \rho \geqslant 0\,,\ \int_{\mathbb{R}^3} \rho\, dx = \mathrm{N} \right\}\,.$$

Soulignons que, contrairement à la théorie de Schrödinger, le modèle de Thomas-Fermi est une théorie non linéaire. L'importante caractéristique simplificatrice dans le modèle de Thomas-Fermi est qu'on optimise sur des fonctions de seulement trois variables, contrairement aux fonctions de 3N variables dans la théorie de Schrödinger.

Alors que le modèle de Thomas-Fermi existait et était utilisé depuis longtemps, ce n'est que dans les années soixante-dix que Lieb et Simon en ont établi rigoureusement les fondements mathématiques [40]. Ils ont répondu notamment aux questions concernant l'existence et l'unicité des solutions, leur régularité et leur décroissance. Plus tard, Lieb et ses collaborateurs ont étudié de manière systématique les théories de la

fonctionnelle de la densité, qui sont des raffinements du modèle de Thomas-Fermi. Ces résultats sont résumés dans la synthèse [17].

Un autre résultat fondamental que Lieb et Simon démontrent dans leur article sur le modèle de Thomas-Fermi est une relation rigoureuse entre l'énergie de l'état fondamental du hamiltonien H dans l'équation (1) et l'énergie minimale de Thomas-Fermi dans la limite où $N \to \infty$ et $Z \to \infty$ avec $N/Z \to \lambda \in]0, +\infty[$ [*]. Ils démontrent que

$$\lim \frac{\inf \operatorname{spec} H}{\inf \mathcal{E}} = 1 .$$

Cette convergence des énergies est complétée par des résultats de convergence des densités à une particule des états fondamentaux (approximatifs) du hamiltonien de Schrödinger. Ce résultat est techniquement lié à l'analyse semi-classique, mais en dehors des hypothèses de régularité typiques de cette théorie. Le résultat de Lieb et Simon est devenu un modèle pour obtenir d'autres théories effectives dans des limites d'échelle.

Mentionnons également en passant la première démonstration par Lieb et Simon de l'existence de solutions aux équations de Hartree-Fock pour les atomes et les molécules [39]. La théorie de Hartree-Fock est une approximation plus précise de la théorie de Schrödinger que la théorie de Thomas-Fermi. Elle est utilisée dans le calcul des énergies atomiques et moléculaires. Contrairement à la théorie de Thomas-Fermi, qui est une théorie de la fonctionnelle de la densité où l'inconnue est une fonction scalaire, la théorie de Hartree-Fock est une théorie de la matrice densité, où l'inconnue est un opérateur. L'article de Lieb et Simon est un article fondateur du calcul des variations non commutatif.

Dans la théorie de Thomas-Fermi, la répulsion coulombienne entre les électrons est approchée par la quantité $D[\rho]$. Lieb et Oxford [34] ont trouvé en 1981 un minorant pour la différence entre ces deux quantités : c'est l'inégalité de Lieb-Oxford pour l'énergie d'échange. Cette inégalité est bien connue des spécialistes de chimie quantique. Elle guide leurs réflexions sur l'énergie de corrélation d'échange dans les molécules.

Lieb a publié en 1983 un article sur les fonctionnelles de la densité pour les systèmes coulombiens [20] qui a jeté les bases théoriques de la théorie de la fonctionnelle de la densité et qui est fréquemment cité. Cet article introduit une fonctionnelle universelle, connue sous le nom de fonctionnelle de Levy-Lieb, qui donne l'énergie la plus basse qui

*. Nous considérons ici, pour des raisons de simplicité, le cas atomique $K = 1$ et posons $Z = Z_1$. Le cas le plus important est $N = Z$, c'est-à-dire le cas d'un atome neutre.

peut être atteinte lorsque tous les états quantiques possibles ont une fonction de densité donnée. Cette fonctionnelle donne par définition l'énergie de l'état fondamental des systèmes quantiques coulombiens en interaction (même si elle n'est pas connue explicitement). Ce point de vue a joué un rôle très important. La théorie de la fonctionnelle de la densité a explosé dans les années quatre-vingt-dix. Elle est largement utilisée dans l'industrie. C'est désormais la méthode de choix pour calculer l'état quantique des molécules et des solides.

Parmi les travaux les plus récents de Lieb dans cette direction, on peut citer une justification mathématique rigoureuse de l'approximation de la densité locale dans la théorie de la fonctionnelle de la densité, et une démonstration de l'équivalence dans la limite thermodynamique de trois définitions différentes de l'énergie minimale d'un gaz d'électrons homogène. Il s'agit de travaux en collaboration avec Lewin et Seiringer [12, 13].

1.4 Les inégalités de Lieb-Thirring

L'aspect le moins évident de l'approximation de la fonctionnelle d'énergie de Schrödinger par la fonctionnelle de Thomas-Fermi est sans doute le fait que l'énergie cinétique correcte

$$\int_{\mathbb{R}^3} \cdots \int_{\mathbb{R}^3} \sum_{n=1}^{N} |\nabla_n \psi|^2 \, dx_1 \dots dx_N$$

soit remplacée par le terme

$$\gamma^{TF} \int_{\mathbb{R}^3} \rho(x)^{\frac{5}{3}} \, dx$$

pour une certaine constante explicite $\gamma^{TF} > 0$. C'est à cette étape (et seulement à cette étape) de l'approximation que la nature fermionique de la fonction d'onde ψ entre en jeu. Derrière cette approximation se trouve l'observation que l'énergie cinétique par unité de volume d'un gaz de Fermi sans interaction dans son état fondamental avec une densité constante ρ est $\gamma^{TF}\rho^{\frac{5}{3}}$. En imaginant que les particules décrites par une fonction d'onde ψ de faible énergie soient localement essentiellement dans l'état fondamental du gaz de Fermi avec la densité locale correspondante, on arrive à l'expression de Thomas-Fermi pour l'énergie cinétique.

La question se pose de savoir si cette approximation peut être étayée par des inégalités rigoureuses. C'est ce que permet la célèbre inégalité de Lieb-Thirring, qui était un ingrédient crucial dans leur démonstration de la stabilité de la matière [43]. Cette inégalité stipule que pour tout ψ antisymétrique et normalisé sur $\mathbb{R}^{3N}$, on a

$$\int_{\mathbb{R}^3} \cdots \int_{\mathbb{R}^3} \sum_{n=1}^{N} |\nabla_n \psi|^2 \, dx_1 \ldots dx_N \geqslant K \int_{\mathbb{R}^3} \rho_\psi(x)^{\frac{5}{3}} \, dx \tag{3}$$

avec $\rho_\psi(x)$ qui est égal à

$$\sum_{n=1}^{N} \int_{\mathbb{R}^3} \cdots \int_{\mathbb{R}^3} |\psi(x_1, \ldots, x_{n-1}, x, x_{n+1}, \ldots, x_N)|^2 \, dx_1 \cdots dx_{n-1} \, dx_{n+1} \cdots dx_N \, .$$

Le point important ici est que la constante K soit indépendante de N.

L'inégalité de Lieb-Thirring (3) peut être considérée comme une expression mathématique des principes d'exclusion et d'incertitude en mécanique quantique. Le lien avec le principe d'exclusion est que la constante K est indépendante de N ; si les fonctions symétriques ψ (qui décrivent un système bosonique) étaient autorisées, la constante K dans l'inégalité (3) devrait se détériorer avec N (il suffit par exemple de prendre pour ψ une fonction produit $\varphi(x_1) \cdots \varphi(x_N)$). Pour $N = 1$, l'inégalité de Lieb-Thirring se réduit à une certaine inégalité d'interpolation de Sobolev. Pour $N \geqslant 2$, elle peut être considérée comme une généralisation de celle-ci. La conclusion des inégalités de type Sobolev, à savoir qu'un espace L^p avec un « grand » p peut être contrôlé, est un résultat de non-concentration et quantifie par conséquent le principe d'incertitude en mécanique quantique.

La constante K dans l'inégalité (3) que Lieb et Thirring ont obtenue était plus petite que γ^{TF}, mais elle conservait la caractéristique importante d'être indépendante de N (et de ψ bien sûr). La célèbre conjecture de Lieb-Thirring stipule que l'inégalité devrait être valide avec une constante égale à γ^{TF}. Cela signifierait que l'approximation de Thomas-Fermi pour l'énergie cinétique est un minorant universel de son expression de Schrödinger. Cette constante a fait l'objet de nombreux travaux, qui ont abouti au meilleur minorant actuel de $0{,}7785\,\gamma^{TF}$.

Lieb et Thirring n'ont pas démontré directement l'inégalité (3). Ils ont d'abord montré qu'elle était équivalente à une certaine inégalité concernant des sommes de valeurs propres négatives d'opérateurs de Schrödinger à un corps. Ils ont ensuite vérifié cette dernière inégalité.

Dans leur article suivant [44], ils ont étendu cette dernière inégalité à des dimensions arbitraires et à des puissances arbitraires de valeurs propres. Ils ont démontré que les valeurs propres négatives (E_j) de l'opérateur de Schrödinger $-\Delta + V$ dans $L^2(\mathbb{R}^d)$ vérifient

$$\sum_j |E_j|^\gamma \leqslant L_{\gamma,d} \int_{\mathbb{R}^d} V(x)_-^{\gamma+d/2}\, dx$$

pour tout $\gamma > 1/2$ si $d = 1$ et pour tout $\gamma > 0$ si $d \geqslant 2$. Pour $\gamma = 1$ et $d = 3$, cette inégalité est équivalente à l'inégalité (3). Peu après, Lieb [16] a démontré l'inégalité correspondante pour $\gamma = 0$, connue sous le nom d'inégalité de Cwikel-Lieb-Rozenblum, à savoir

$$\#\left\{j :\ E_j < 0\right\} \leqslant L_{0,d} \int_{\mathbb{R}^d} V(x)_-^{d/2}\, dx$$

pour $d \geqslant 3$.

La forme générale de la célèbre conjecture de Lieb-Thirring concerne les valeurs optimales des constantes $L_{\gamma,d}$. Outre l'importance évidente des valeurs de ces constantes dans les applications, la conjecture aborde à un niveau conceptuel la force du principe d'exclusion dans différentes dimensions. Lieb, en collaboration avec Hundertmark et Thomas, a démontré le seul cas connu d'inégalité optimale où la constante n'est pas donnée par celle provenant d'une approximation semi-classique (ou de type Thomas-Fermi). De plus, après plus de quarante ans, la valeur de la constante $L_{0,3}$ donnée par Lieb est toujours la plus petite connue.

Les inégalités de Lieb-Thirring et de Cwikel-Lieb-Rozenblum et leurs généralisations sont d'une grande importance dans l'étude des grands systèmes fermioniques. Elles ont trouvé en outre des applications dans le contexte des équations d'évolution non linéaires telles que les équations de Navier-Stokes. Elles ont aussi suscité un grand intérêt d'un point de vue purement mathématique. Le fait que l'orthogonalité de fonctions conduise à une dépendance améliorée sur le nombre de fonctions a été vérifié dans un certain nombre d'autres inégalités fonctionnelles [9, 18].

1.5 Le problème de l'ionisation

Revenons au hamiltonien quantique à plusieurs corps H dans l'équation (1). La borne inférieure de son spectre peut être ou non

une valeur propre. Si c'est le cas, nous interprétons la fonction propre correspondante comme décrivant l'état fondamental du système et nous considérons que les N électrons sont liés aux noyaux. L'intuition physique suggère que des noyaux donnés avec des charges données ne peuvent se lier qu'avec un nombre fini d'électrons, mais même cela n'est pas tout à fait évident d'un point de vue mathématique. La version quantitative de cette question, à savoir le nombre d'électrons avec lequel un atome (ou une molécule) peut se lier, n'est toujours pas réglée malgré de sérieux efforts.

Pour simplifier, limitons notre attention au cas atomique avec K = 1 dans l'équation (1). Les données expérimentales et les estimations numériques montrent qu'un noyau de charge Z ne peut se lier qu'avec au plus Z + 1 voire Z + 2 électrons. Démontrer (ou réfuter) cela rigoureusement dans le modèle de Schrödinger ci-dessus est un célèbre problème ouvert.

L'un des rares résultats non asymptotiques dans cette direction est dû à Lieb [23] et stipule qu'un noyau atomique ne peut pas se lier avec 2Z + 1 électrons ou plus. Le facteur 2 devant Z semble « trop grand » pour les grandes valeurs de Z. Mais par exemple pour Z = 1, la borne est optimale. Ce n'est que trois décennies plus tard que le résultat de Lieb a été amélioré pour les grandes valeurs de Z.

Une découverte frappante de Benguria et Lieb [2] est que la borne supposée sur la charge excédentaire ne serait pas vraie si les électrons étaient des bosons, c'est-à-dire si la condition d'antisymétrie sur les fonctions admissibles était remplacée par la condition de symétrie $\psi(\ldots, x_n, \ldots, x_m, \ldots) = \psi(\ldots, x_m, \ldots, x_n, \ldots)$ pour tout $n \neq m$. Ils ont montré qu'il existe un nombre $\lambda > 1$ (numériquement $\lambda \approx 1{,}21$) tel qu'un « atome bosonique » pourrait se lier avec au moins $(\lambda + o(1))Z$ électrons quand $Z \to \infty$. En conséquence du résultat de Benguria et Lieb, le principe d'exclusion de Pauli (c'est-à-dire l'exigence d'antisymétrie) doit intervenir dans toute démonstration éventuelle. Cela exclut en particulier tout argument naïf purement électrostatique.

Pour revenir au cas fermionique original, on peut se demander s'il y a au moins une neutralité asymptotique dans le sens où, lorsque $Z \to \infty$, le nombre d'électrons qui peuvent être liés est $Z + o(Z)$. Lieb, Sigal, Simon et Thirring ont démontré que c'était effectivement le cas [38]. D'autres chercheurs ont obtenu par la suite des bornes quantitatives sur le reste $o(Z)$. Mais montrer qu'il est borné semble être hors de portée des techniques actuelles.

1.6 Les systèmes bosoniques

Bien que nous nous concentrions principalement dans cette section sur les systèmes fermioniques, Lieb a également apporté de nombreuses contributions fondamentales à l'étude des systèmes bosoniques. Parmi ces contributions, on peut citer les suivantes :

1. La construction, avec Liniger, d'un modèle de gaz de Bose unidimensionnel en interaction [31]. Ce modèle a servi de prototype pour les développements théoriques ultérieurs. Il a également été réalisé expérimentalement.

2. Avec Yngvason, Lieb a démontré une formule asymptotique, conjecturée cinquante-huit ans plus tôt, pour l'énergie de l'état fondamental d'un gaz de Bose dilué [45]. Par la suite, avec Seiringer et Yngvason, il a rigoureusement établi l'équation de Gross-Pitaevskii pour l'énergie de l'état fondamental des bosons dilués dans un piège, en partant de la mécanique quantique à plusieurs corps [36]. Ce résultat a eu un impact considérable sur le développement de la physique mathématique au cours des deux dernières décennies.

3. Avec Conlon et Yau [7] et plus tard avec Solovej [41, 42], Lieb a démontré une loi en $N^{7/5}$ pour les bosons chargés. Cela signifie en gros que l'énergie n'obéit pas à une inégalité linéaire comme dans l'inégalité (2), mais qu'elle décroît plutôt comme $-CN^{7/5}$. Il s'agit de la première validation rigoureuse de la théorie d'appariement de Bogolioubov pour le gaz de Bose, qui a ouvert la voie à de nombreux développements actuels.

2 Les inégalités fonctionnelles

Le nom de Lieb est indissociable du sujet des inégalités. Un volume entier de 700 pages de ses « Œuvres choisies » est consacré à ce sujet [26]. Dans la section précédente, lors de l'examen de l'inégalité de Lieb-Thirring, nous avons déjà vu un exemple d'inégalité fonctionnelle. Dans cette section, nous examinerons trois autres exemples, à savoir les inégalités d'entropie en analyse matricielle, les inégalités de Brascamp-Lieb et la forme optimale de l'inégalité de Hardy-Littlewood-Sobolev.

2.1 Le théorème de concavité de Lieb et la sous-additivité forte

En 1973, Lieb et Ruskai ont démontré la *sous-additivité forte de l'entropie quantique* [35]. Ce théorème a de nombreuses formulations équivalentes, telles que la concavité de l'entropie conditionnelle, la convexité conjointe de l'entropie relative ou la monotonie de l'entropie relative. La sous-additivité forte, ou l'un de ses équivalents, joue un rôle essentiel dans le domaine moderne et très actif de l'information quantique et des ordinateurs quantiques.

Énonçons ce théorème dans sa formulation de monotonie, obtenue à l'origine par Lindblad en 1974 à partir d'un résultat de Lieb. Une matrice densité est une matrice hermitienne positive de trace égale à 1. L'entropie relative (ou divergence de Kullback-Leibler) de deux matrices densités ρ et σ est définie par

$$\mathrm{D}(\rho\|\sigma) = \operatorname{Tr}\rho\ln\rho - \operatorname{Tr}\rho\ln\sigma\,.$$

Ce nombre est positif ou nul. Il est nul si et seulement si $\rho = \sigma$. Il mesure en gros à quel point ρ et σ sont distinguables, même s'il n'est pas symétrique en ρ et σ. Les opérations quantiques sont décrites par des applications complètement positives qui préservent la trace. Le théorème de monotonie de l'entropie relative (également connu sous le nom d'*inégalité de traitement des données*) stipule que pour toute opération $\mathcal{E}$ de ce type, on a

$$\mathrm{D}(\mathcal{E}\rho\|\mathcal{E}\sigma) \leqslant \mathrm{D}(\rho\|\sigma)\,.$$

Ainsi, l'application d'une opération quantique ne peut que rendre les états plus difficiles à distinguer. Il est donc clair que la monotonie de l'entropie relative est à la base même de la théorie de l'information quantique.

La démonstration par Lieb et Ruskai de la sous-additivité forte de l'entropie et la démonstration par Lindblad de la monotonie de l'entropie relative reposent toutes deux sur un théorème profond que Lieb a démontré dans son article de 1973 sur les « fonctions traces convexes et la conjecture de Wigner-Yanase-Dyson » [14]. Ce théorème stipule que pour tout $p, q \geqslant 0$ avec $p + q \leqslant 1$, l'application $(\mathrm{A}, \mathrm{B}) \mapsto \operatorname{Tr}\mathrm{A}^p\mathrm{B}^q$ définie sur les matrices hermitiennes positives est conjointement concave.

L'article de Lieb a donné lieu à de nombreux travaux ultérieurs qui contiennent d'autres démonstrations, généralisations et applications. Lui-même, souvent en collaboration avec Carlen, est revenu à plusieurs

reprises sur ce thème et a approfondi notre compréhension de l'analyse matricielle ; voir par exemple [1, 6].

2.2 Les inégalités de Brascamp-Lieb

En 1976, Brascamp et Lieb ont publié un article sur « les meilleures constantes dans l'inégalité de Young, son inverse et sa généralisation à plus de trois fonctions » [3]. Cet article traite de trois sujets liés mais différents. Il est célèbre pour chacun d'entre eux.

Le premier sujet concerne une inégalité fondamentale en analyse réelle, à savoir l'inégalité de Young

$$\left| \iint_{\mathbb{R}^d \times \mathbb{R}^d} f(x) g(x-y) h(y)\, dx\, dy \right| \leqslant C_{p,q,r,d}\, \|f\|_{L^p(\mathbb{R}^d)}\, \|g\|_{L^q(\mathbb{R}^d)}\, \|h\|_{L^r(\mathbb{R}^d)} \quad (4)$$

pour trois fonctions f, g, h sur $\mathbb{R}^d$ et des paramètres $1 \leqslant p, q, r \leqslant \infty$ qui vérifient $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 2$. Cette inégalité apparaît fréquemment dans la théorie et les applications, car la convolution est une opération de base en analyse mathématique. L'inégalité de Young mesure son effet dans les espaces de Lebesgue.

La question est de trouver la constante optimale (c'est-à-dire la plus petite possible) $C_{p,q,r,d}$ dans l'inégalité (4) et de caractériser tous les cas d'égalité. Le premier objectif a été atteint par Beckner à peu près en même temps que [3]. Brascamp et Lieb ont trouvé une démonstration alternative et ont atteint le second objectif. Leur démonstration combine de manière originale la technique du réarrangement symétrique décroissant avec des produits tensoriels, ce qui conduit à un résultat de convergence dans l'esprit du théorème central limite. Il s'ensuit que la constante optimale est déterminée par les fonctions gaussiennes et n'est atteinte que pour celles-ci.

Le second sujet de l'article de Brascamp et Lieb est que l'inégalité de Young est valable avec le signe de l'inégalité inversé si $0 < p, q \leqslant 1$ et si f, g, h sont positifs ou nuls. Là encore, les auteurs ont été en mesure de calculer la constante optimale. Cette inégalité de Young inversée contient comme cas limite le théorème de Prékopa-Leindler.

Le troisième sujet de l'article de Brascamp et Lieb est une généralisation importante de l'inégalité de Young à un nombre arbitraire de fonctions, ainsi qu'un remplacement des fonctions linéaires x, y et $x - y$ sur $\mathbb{R}^{2d}$ qui apparaissent dans l'inégalité (4) par une classe beaucoup plus large de fonctions linéaires. La famille d'inégalités qui en résulte est maintenant connue sous le nom d'inégalités de Brascamp-Lieb.

Elle contient non seulement l'inégalité de Young, mais aussi l'inégalité de Hölder et celle de Loomis-Whitney en tant que cas particuliers. Brascamp et Lieb montrent que pour des applications linéaires données, l'inégalité est valable avec une constante finie si et seulement si elle est valable pour les fonctions gaussiennes. Dans ce cas, la constante optimale peut être calculée en utilisant cette dernière classe de fonctions. Leur argument est à nouveau basé sur un théorème central limite.

Outre leur application originale à la physique statistique, les inégalités de Brascamp-Lieb ont joué un rôle important dans la théorie de la convexité, l'analyse harmonique et d'autres domaines des mathématiques.

Dans son article de 1990 sur « les noyaux gaussiens qui n'ont que des maximiseurs gaussiens » [24], Lieb revient sur le sujet des inégalités de Young et de Brascamp-Lieb. Il démontre un théorème général sur la norme d'une grande classe d'opérateurs intégraux. Entre autres choses, il caractérise les cas d'égalité dans l'inégalité de Hausdorff-Young avec une constante optimale. Là encore, ils sont donnés par des fonctions gaussiennes.

Mentionnons enfin qu'il existe une autre inégalité célèbre connue sous le nom d'inégalité de Brascamp-Lieb. Il s'agit d'une inégalité de Poincaré (ou de trou spectral) pour les lois de probabilité logarithmiquement concaves [4].

2.3 L'inégalité de Hardy-Littlewood-Sobolev optimale

Un résultat fondamental de l'analyse réelle, connu sous le nom d'inégalité de Hardy-Littlewood-Sobolev, d'inégalité faible de Young ou de théorème d'intégration fractionnaire, stipule que pour tout $0 < \lambda < d$ et pour tout $1 < p, r < \infty$ avec $\frac{1}{p} + \frac{\lambda}{d} + \frac{1}{r} = 2$, on a

$$\left| \iint_{\mathbb{R}^d \times \mathbb{R}^d} \frac{f(x)\, h(y)}{|x-y|^\lambda}\, dx\, dy \right| \leqslant C_{\lambda,p,r}\, \|f\|_{L^p(\mathbb{R}^d)}\, \|h\|_{L^r(\mathbb{R}^d)}\,. \tag{5}$$

Cette inégalité a de nombreuses applications en mathématiques pures et appliquées. Par exemple, dans le cas où $\lambda = d - 2$ et $d \geqslant 3$, le noyau de cette inégalité est le noyau de Coulomb et la quantité du côté gauche représente l'interaction coulombienne de deux densités de charge f et g. Pour $\lambda = d - 2$ et $p = r$, l'inégalité (5) est équivalente à l'inégalité de Sobolev.

L'article de Lieb de 1983 sur « les constantes optimales dans les inégalités de Hardy-Littlewood-Sobolev (HLS) et les inégalités connexes » [19]

a eu un impact profond sur le domaine du calcul des variations. En effet, cet article et son article associé de 1983 sur « une relation entre la convergence ponctuelle des fonctions et la convergence des fonctionnelles » [5] avec Brezis sont les articles de mathématiques pures les plus cités de Lieb.

L'article sur les constantes optimales est remarquable pour au moins deux aspects distincts, à savoir le développement d'un argument de compacité assez général et une observation ingénieuse concernant le problème en question. Nous discutons brièvement de ces deux points.

L'aspect compacité de l'article HLS de Lieb concerne la question de savoir s'il existe un couple non trivial (f, h) tel que l'égalité dans (5) ait lieu avec la constante $C_{\lambda,p,r}$ minimale. Lieb avait déjà travaillé sur des questions relatives à l'existence d'optimiseurs pour certains problèmes variationnels. Contrairement aux problèmes variationnels classiques, ces problèmes sont souvent invariants par translation. Lieb a donc dû trouver des méthodes pour traiter la perte de compacité correspondante (par exemple par un réarrangement symétrique décroissant [15] ou par un « argument de poursuite » original [21]). Le problème d'optimisation pour l'inégalité HLS présente cependant une autre perte potentielle de compacité, à savoir à travers les dilatations. Afin de traiter ces problèmes, Lieb a trouvé un renforcement du lemme de Fatou, qui dit que si des fonctions f_j sur un espace mesuré X sont bornées dans L^p et convergent ponctuellement presque partout vers une fonction f, alors

$$\lim_{j\to\infty} \int_X \left| |f_j|^p - |f|^p - |f_j - f|^p \right| dx = 0 \,. \tag{6}$$

En particulier,

$$\int_X |f_j|^p \, dx = \int_X |f|^p \, dx + \int_X |f_j - f|^p \, dx + o(1) \,.$$

À titre de comparaison, dans le lemme de Fatou, le deuxième terme du second membre est omis, ce qui conduit à une inégalité plutôt qu'à une égalité. La relation (6) avec $|\cdot|^p$ remplacé par des fonctions plus générales est connu sous le nom de lemme de Brezis-Lieb et constitue un outil fondamental en analyse fonctionnelle et en calcul des variations.

La méthode de compacité de Lieb, parfois appelée méthode de la masse manquante, suit attentivement le terme résiduel $f_j - f$ dans l'équation (6). Cette technique est assez robuste et a trouvé diverses applications dans différents contextes, y compris dans [11]. D'autres

méthodes de compacité utilisent également le lemme de Brezis-Lieb comme ingrédient fondamental.

Le deuxième aspect remarquable de l'article HLS de Lieb concerne le cas particulier $p = r$ (mais où $0 < \lambda < d$ est arbitraire). Lieb a réussi à calculer explicitement la plus petite constante possible $C_{\lambda,p,r}$ et à caractériser tous les couples de fonctions (f, h) pour lesquels il y a égalité. L'observation cruciale dans la démonstration de Lieb était une symétrie « cachée », à savoir l'invariance conforme de (5) pour $p = r$. L'article de Lieb a donné naissance à un champ de problèmes variationnels avec invariance conforme. Parmi ces développements figure également la forme optimale de l'inégalité HLS sur le groupe de Heisenberg [10].

3 Sujets non couverts

Dans les sections précédentes, nous avons abordé deux thèmes de l'œuvre de Lieb, à savoir les systèmes quantiques coulombiens et les inégalités fonctionnelles. Ces sujets ne représentent qu'une fraction de l'ensemble des travaux de Lieb. Il est probable que d'autres auteurs auraient choisi des sujets complètement différents. Nous manquerions à notre devoir si nous ne mentionnions pas au moins brièvement quelques autres sujets.

Nous avons complètement ignoré le chapitre important des modèles intégrables dans les travaux de Lieb des années soixante. Ce domaine a été révolutionné par les solutions de Lieb du modèle à six sommets, du modèle F de Fierz-Rys et du modèle KDP de Slater, ainsi que du modèle de Lieb-Liniger déjà mentionné. En relation avec le modèle à six sommets, Lieb et Temperley ont construit ce qui est devenu l'algèbre de Temperley-Lieb, qui a des applications dans plusieurs domaines des mathématiques, par exemple en théorie des nœuds, et en physique. Les travaux de Lieb sont à la base de la physique statistique moderne et ont une influence durable sur les probabilités intégrables et la combinatoire, entre autres.

Concernant les contributions de Lieb à la physique de la matière condensée, Nachtergaele, Solovej et Yngvason écrivent dans la préface du troisième volume des « Œuvres choisies » de Lieb [28] :

> « L'impact des travaux de Lieb dans le domaine de la physique mathématique de la matière condensée est inégalé. On peut dire que si l'on devait nommer un père fondateur

> de ce domaine, Elliott Lieb serait le seul candidat à pouvoir prétendre à cette position singulière. »

Ce domaine comprend notamment les travaux fondamentaux de Lieb sur le modèle de Hubbard, y compris sa solution dans le cas unidimensionnel avec Wu et la découverte du ferromagnétisme de Lieb et du réseau de Lieb, ainsi que les travaux très cités réalisés en collaboration avec Schultz et Mattis sur deux modèles résolubles de chaîne antiferromagnétique et avec Mattis sur le modèle de Luttinger et la découverte de la bosonisation.

Dans l'introduction, nous avons déjà mentionné les « bornes de Lieb-Robinson », qui établissent le fait profond qu'il existe une vitesse de groupe finie pour la propagation de l'information dans les systèmes de spins quantiques. Cela s'est avéré très important pour les idées sur l'informatique quantique et la physique de la matière condensée.

Lieb a développé en outre avec Affleck, Kennedy et Tasaki ce que l'on a appelé le modèle AKLT d'une chaîne de spins de spin égal à 1. Ce modèle s'est avéré être un prototype important d'une classe de modèles et d'états propres connus sous le nom d'états de produits matriciels.

Dans le domaine de la physique statistique, mentionnons la démonstration par Lieb de l'existence de transitions de phase dans les systèmes de spins classiques et quantiques, obtenue conjointement avec Fröhlich, Israel et Simon et avec Dyson et Simon. Les démonstrations reposent sur la méthode de la positivité par réflexion, que Lieb a magistralement utilisée dans plusieurs situations.

Un autre résultat célèbre est le travail de Lieb avec Heilman sur les zéros de la fonction de partition du problème monomère-dimère, qui est lié au problème d'appariement en combinatoire. Ce résultat est également important en informatique.

Une nouvelle approche de la physique et des mathématiques du deuxième principe de la thermodynamique, développée conjointement avec Yngvason, mérite d'être mentionnée.

La liste des sujets abordés dans cette section s'est jusqu'à présent concentrée sur les travaux de Lieb les plus axés sur la physique. En ce qui concerne les travaux plus orientés vers les mathématiques, mentionnons simplement ses contributions fondamentales à la théorie du réarrangement symétrique décroissant. Cela inclut notamment une inégalité générale de réarrangement pour de nombreuses fonctions, obtenue avec Brascamp et Luttinger, ainsi que la démonstration obtenue avec Almgren que le réarrangement symétrique décroissant peut être discontinu dans les espaces de Sobolev.

Enfin, nous aimerions mentionner le livre de Lieb et Loss [32], qui est devenu un manuel de référence pour les cours d'analyse de troisième cycle et qui promeut de manière éloquente et concise la philosophie des mathématiques rigoureuses en vue des applications.

Nous espérons que ces pages seront une invitation à consulter les articles de recherche originaux de Lieb. Ce n'est qu'ainsi que le lecteur pourra ressentir la clarté, la vitalité et la beauté de l'œuvre de Lieb, une œuvre qui a inspiré et continue d'inspirer des générations.

Félicitations Elliott pour l'obtention du prix Gauss !

Financement. Nous remercions la Fondation nationale des sciences des États-Unis pour son soutien (DMS-1954995) ainsi que la Fondation allemande pour la recherche et sa stratégie d'excellence allemande (EXC-2111-390814868). L'auteur remercie M. Lewin pour ses remarques utiles.

Bibliographie

[1] *Invent. math.*, nº 115, 1994, p. 463-482.

[2] *Phys. Rev. Lett.*, nº 50, 1983, p. 1771–1774.

[3] *Adv. Math.*, nº 20, 1976, p. 151-172.

[4] *J. Funct. Anal.*, nº 22, 1976, p. 366-389.

[5] *Proc. Am. Math. Soc.*, nº 88, 1983, p. 486-490.

[6] *Differential Operators and Spectral Theory*, American Mathematical Society, 1999, p. 59-69.

[7] *Commun. Math. Phys.*, nº 116, 1988, p. 417-448.

[8] *The Physics and Mathematics of Elliott Lieb : The 90th Anniversary*, Berlin, EMS Press, 2022.

[9] *J. Eur. Math. Soc.*, nº 16, 2014, p. 1507-1526.

[10] *Ann. Math.*, nº 176, 2012, p. 349-381.

[11] *Geom. Funct. Anal.*, nº 26, 2016, p. 1095-1134.

[12] *J. Éc. polytech. Math.*, nº 5, 2018, p. 79-116.

[13] *Pure Appl. Anal.*, nº 2, 2020, p. 35-73.

[14] *Adv. Math.*, nº 11, 1973, p. 267-288.

[15] *Stud. Appl. Math.*, nº 57, 1977, p. 93-105.

[16] *Geometry of the Laplace Operator*, American Mathematical Society, 1980, p. 241-252.

[17] *Rev. Mod. Phys.*, nº 53, 1981, p. 603-641.

[18] *J. Funct. Anal.*, nº 51, 1983, p. 159-165.

[19] *Ann. Math.*, nº 118, 1983, p. 349-374.

[20] *Int. J. Quant. Chem.*, nº 24, 1983, p. 243-277.

[21] *Invent. math.*, nº 74, 1983, p. 441-448.

[22] *Commun. Math. Phys.*, nº 92, 1984, p. 473-480

[23] *Phys. Rev. A*, nº 29, 1984, p. 3018-3028.

[24] *Invent. math.*, nº 102, 1990, p. 179-208.

[25] *Bull. Am. Math. Soc.*, nº 22, 1990, p. 1-49.

[26] Lieb (Elliott H.), *Inequalities, Selecta of Elliott H. Lieb*, Springer, 2002.

[27] Lieb (Elliott H.), *Statistical Mechanics, Selecta of Elliott H. Lieb*, Springer, 2004.

[28] Lieb (Elliott H.), *Condensed Matter Physics and Exactly Soluble Models, Selecta of Elliott H. Lieb*. Springer, 2004.

[29] Lieb (Elliott H.), *The Stability of Matter : from Atoms to Stars. Selecta of Elliott H. Lieb*, 4e éd., Springer, 2005.

[30] *Adv. Math.*, nº 9, 1972, p. 316-398.

[31] *Phys. Rev.*, nº 130, 1963, p. 1605-1616.

[32] Lieb (Elliott H.) et Loss (Michael), *Analysis*, 2e éd., American Mathematical Society, 2001.

[33] *Phys. Rev. Lett.*, nº 75, 1995, p. 985-989.

[34] *Int. J. Quant. Chem.*, nº 19, 1981, p. 427-439.

[35] *J. Math. Phys.*, nº 14, 1973, p. 1938-1941.

[36] *Phys. Rev. A*, nº 61, 2000, article 043602.

[37] Lieb (Elliott H.) et Seiringer (Robert), *The Stability of Matter in Quantum Mechanics*. Cambridge University Press, 2010.

[38] *Commun. Math. Phys.*, nº 116, 1988, p. 635-644.

[39] *Commun. Math. Phys.*, nº 53, 1977, p. 185-194.

[40] *Adv. in Math.*, nº 23, 1977, p. 22-116.

[41] *Commun. Math. Phys.*, nº 217, 2001, p. 127-163 ; erratum, *ibid.*, nº 225, 2002, p. 219-221.

[42] *Commun. Math. Phys.*, nº 252, 2004, p. 485-534.

[43] *Phys. Rev. Lett.*, nº 35, 1975, p. 687-689 ; erratum, *ibid.*, p. 1116.

[44] *Studies in Mathematical Physics*, Princeton University Press, 1976, p. 269-303.

[45] *Phys. Rev. Lett.*, nº 80, 1998, p. 2504-2507.

Nikolaï Andreïev et l'art de l'animation mathématique et de la construction de modèles (par Tadashi Tokieda)

Le prix Līlāvatī de l'Union mathématique internationale a été décerné lors du congrès international des mathématiciens de 2022 à Nikolaï Andreïev pour avoir développé l'animation mathématique et la construction de modèles mathématiques dans un style qui inspire les jeunes et les moins jeunes et que les mathématiciens du monde entier peuvent adapter à leurs diverses utilisations, ainsi que pour ses efforts inlassables pour vulgariser des mathématiques sérieuses auprès du public.

Dans le domaine des mathématiques visuelles et tactiles, Nikolaï Nikolaïevitch Andreïev est passé maître dans l'art merveilleux de l'animation et de la construction de modèles. L'animation diffère de la simulation : il s'agit d'une vidéo ludique d'une histoire qui se déroule sous nos yeux et qui provoque une surprise mathématique agréable à regarder. Les modèles diffèrent de l'impression 3D : ils sont fabriqués à la main, en bois ou en papier, et sont agréables à toucher et à manipuler. Ses animations et ses modèles sont minimalistes mais exécutés avec un savoir-faire consommé. Le style caractéristique d'Andreïev capte l'imagination des jeunes et des moins jeunes et offre des possibilités d'utilisation variées pour la vulgarisation des mathématiques. Parallèlement, il est reconnu pour sa formidable résilience, car il a souvent surmonté des épreuves pour continuer à susciter l'enthousiasme pour les mathématiques auprès d'un grand nombre de personnes de toutes conditions par le biais de ressources en ligne, de conférences et d'un livre. C'est pour cela qu'il reçoit le prix Līlāvatī 2022.

L'Europe de l'Est a une tradition bien ancrée, qui remonte à l'époque de Tchebychev, d'organisation au niveau national d'activités mathématiques qui vont des petits enfants aux étudiants. Certaines de ces activités ont été exportées à l'étranger, comme en témoignent les « cercles mathématiques » qui fleurissent aujourd'hui dans des centres d'initiative à travers le monde. C'est de cette tradition qu'est né *Kvant*,

Tokieda (Tadashi), « Nikolai Andreev and the art of mathematical animation and model-building », dans *Proc. Int. Cong. Math. 2022*, vol. I, p. 160-162. DOI 10.4171/ICM2022/215

sans doute le magazine de vulgarisation des mathématiques et de la physique théorique de la plus haute qualité que le monde ait connu, avec un tirage de 2×10^5 à son apogée (un petit frère, *Kvantik* [1], a vu le jour en 2012). C'est dans le cadre de cette tradition qu'Andreïev, ou Kolya pour ses nombreux amis, est né en 1975 à Saratov. C'est de cette tradition qu'il peut prétendre être un successeur de premier plan en ce XXIe siècle.

Il a commencé sa formation en tant que chercheur. Diplômé de la faculté de mécanique et de mathématiques de l'université d'État de Moscou, il a obtenu un doctorat en 2000 dans le domaine des problèmes extrémaux et de la théorie de l'approximation. Il a commencé la même année à travailler à l'institut de mathématiques Steklov, où il est resté depuis.

L'année 2002 a marqué un tournant : Andreïev a réuni une équipe composée de R. A. Kokcharov (développeur principal et concepteur de sites), M. A. Kalinitchenko (graphiste et vidéaste) et N. M. Paniounine (mathématiques) pour démarrer le projet intitulé « Études mathématiques » [2]. Ce projet est un trésor de vidéos d'animation accessibles à tous gratuitement. Chaque vidéo donne une expérience mathématique brève mais sérieuse d'un point intéressant, élémentaire mais peu connu ; ceci contraste avec la pratique courante qui consiste à présenter de manière journalistique un sujet à la mode. Il a également recruté A. D. Lechinski, un sculpteur d'une habileté stupéfiante, qui concrétise des phénomènes mathématiques curieux par de magnifiques modèles en bois. Andreïev a été nommé en 2010 directeur du laboratoire de vulgarisation de l'institut Steklov. Les productions de son laboratoire comprennent, en plus de nouvelles « Études » et de nouveaux modèles en bois, la collection des « mécanismes de Tchebychev » [3], des gadgets mobiles qui font un usage curieux des mathématiques classiques, et le livre « La part mathématique de toute chose » (Математическая

составляющая) [4], une anthologie écrite par une trentaine de mathématiciens sur une variété luxuriante de sujets qui rappellent *Kvant*. Le livre, publié pour la première fois en 2015 en collaboration avec S. P. Konovalov, N. M. Paniounine et R. A. Kokcharov, a obtenu une médaille d'or de la vulgarisation scientifique en 2017. Une deuxième édition, dont le contenu a plus que doublé, a suivi en 2019.



Andreïev a parcouru de long en large un vaste continent pour donner des conférences, plus de mille en vingt ans, s'adressant ainsi à un public innombrable, en particulier aux adolescents. À maintes reprises, son dévouement et sa persévérance extraordinaires lui ont permis de mener à bien ses projets malgré les embûches administratives et financières chroniques, les négociations interminables et les contretemps. Chaque fois que le financement de son équipe se tarissait, il divisait son propre salaire en parts égales entre lui et les autres membres de l'équipe afin de continuer le travail.

Malgré toutes ces réalisations, une grande partie de la carrière d'Andreïev est encore devant lui. Nous remercions Kolya en tant que représentant de la communauté des mathématiciens qui se sont donnés sans compter au fil des siècles pour faire des mathématiques avec chaque nouvelle génération montante. Nous attendons avec impatience d'être stimulés par ses travaux dans les décennies à venir.

Bibliographie

[1] https://kvantik.com
[2] https://etudes.ru
[3] https://tcheb.ru
[4] https://book.etudes.ru

Index

Ce recueil regroupe les traductions en français des éloges des lauréats de la médaille Fields, de la médaille de l'abaque, de la médaille Chern, du prix Gauss et du prix Līlāvatī lors du congrès international des mathématiciens de 2022. Il donne donc un petit aperçu de ce à quoi ressemblent les mathématiques contemporaines.

ISBN : 979-10-426-5384-2

12 €

Éloges des lauréats du congrès international des mathématiciens de 2022