AVRIL 2015 – N° 144

la Gazette des Mathématiciens

- **La révolution des Big Data**
- **Diffusion des savoirs** – Les maths vues par un artiste
- **Parité** – Filières scientifiques d'excellence : un bastion masculin ?
- **Raconte-moi...** le processus SLE

Société Mathématique de France
SMF

la Gazette des Mathématiciens

Comité de rédaction

Secrétariat de rédaction :
SMF – Claire Ropartz
Institut Henri Poincaré
11 rue Pierre et Marie Curie
75231 Paris cedex 05
Tél. : 01 44 27 67 96 – Fax : 01 40 46 90 96
gazette@dma.ens.fr – http://smf.emath.fr

Directeur de la publication : Marc Peigné

ISSN : 0224-8999

Classe LaTeX : Denis Bitouzé (denis.bitouze@lmpa.univ-littoral.fr)

Conception graphique : Nathalie Lozanne (n.lozanne@free.fr)

Impression : Jouve – 1 rue du docteur Sauvé 53100 Mayenne

Nous utilisons la police Kp-Fonts créée par Christophe Caignaert.

Société Mathématique de France
SMF

À propos de la couverture. Il s'agit du tableau « Le petit déjeuner de Poincaré », peint par Reg Alcorn pour l'exposition « Poincaré-Turing (1854-1912-1954) » de l'IREM de Limoges et du CCSTI du Limousin Récréasciences. Plus de détails se trouvent dans l'article en pages intérieures ou sur la toile http://www.irem.unilim.fr/les-maths-vues-par-un-artiste/ (crédit : Reg Alcorn).

la Gazette des Mathématiciens

N° 144

Éditorial

Chères lectrices, chers lecteurs,

Vous avez été nombreux à nous faire parvenir vos réactions concernant cette nouvelle mouture de notre chère *Gazette*. L'équipe de rédaction vous remercie de vos encouragements et nous espérons également que nous saurons prendre en compte vos suggestions de façon satisfaisante. Je profite de de cet éditorial pour saluer Fabrice Planchon, dont le mandat au sein du comité de rédaction prend fin, ainsi que pour souhaiter la bienvenue à Julie Déserti qui nous rejoint.

Les *Big Data*, ou plutôt les *mégadonnées*, semblent être sur toutes les lèvres depuis quelques temps, sans que l'on sache pour autant ce que cette expression signifie précisément. Celles-ci affectent de façon grandissante de nombreux secteurs d'activité et soulèvent de nouvelles questions au confluent des mathématiques et de l'informatique. Afin d'en savoir davantage, la *Gazette* leur consacre un dossier.

Une étude sociologique détaillée sur les biais, aussi bien en termes de genre que d'origines sociales, dans le recrutement des filières scientifiques de l'ÉNS Paris a récemment vu le jour. La rubrique *Parité* en profite pour donner la parole à Arnaud Pierrel, l'un des auteurs de ce rapport.

Et puis des maths bien sûr ! Étudier les équations d'Einstein du vide, partager le secret d'un logarithme discret, ou, signe des temps, grimper aux cimes des arbres pour découvrir… des immeubles.

La rubrique *Raconte-moi* se penche quant-à-elle sur le processus SLE.

Nous revenons enfin dans ces pages sur une initiative originale impliquant l'IREM de Limoges et à laquelle ce numéro doit sa couverture : l'artiste Reg Alcorn vous convie au *petit déjeuner de Poincaré*, une invitation aux mathématiques à travers l'art et son histoire. À table donc !

En vous souhaitant une agréable lecture,

Boris ADAMCZEWSKI

la Gazette des Mathématiciens

N° 144

Sommaire

Société Mathématique de France
SMF
N° 144

Mot du président

Chères collègues, chers collègues,

Je tiens dans un premier temps à féliciter Adrian Langer, premier lauréat du Prix « Szolem Mandelbrojt » créé par l'Institut français de Pologne, l'Ambassade de France en Pologne et la Société Mathématique de France. Ce prix destiné à un jeune chercheur polonais vise à récompenser des travaux d'excellence dans le domaine des mathématiques. Adrian Langer sera accueilli pendant un mois au laboratoire de mathématiques J.A. Dieudonné et effectuera quelques exposés avec le parrainage de la Société Mathématique de France.

Les mois qui viennent de s'écouler ont été marqués par la réflexion autour des nouveaux programmes de collèges et lycées, à laquelle la SMF participe pleinement et dont les médias se sont emparée peu à peu. En lien étroit avec les autres sociétés savantes de mathématiques et la Commission Française de l'Enseignement des Mathématiques (CFEM), la SMF suit le dossier avec attention et participe aux rencontres avec le ministère et le comité des programmes. Ce n'est qu'au printemps que les premières versions « officielles » des programme seront rendues publiques, pour concertation avec l'ensemble des acteurs concernés par ce dossier ; la commission enseignement de la SMF travaille en amont pour se préparer à cette phase de concertation, en étroite collaboration avec les membres de la CFEM.

Le forum « Mathématiques vivantes, de l'école au monde » qui a clôturé avec succès début mars la semaine des mathématiques s'inscrit dans la mobilisation de la communauté mathématique française pour susciter des vocations chez les jeunes générations. Il faisait notamment écho à l'annonce début décembre par la ministre M^me^ Vallaud-Belkacem du plan stratégique pour les mathématiques. À l'occasion de ce Forum est sortie la brochure « Zoom des métiers des mathématiques et de l'informatique », élaborée en étroite concertation par la SMF, la SMAI, la SFDS, la Société Informatique de France, femmes & mathématiques et l'ONISEP. C'est un outil essentiel pour attirer des jeunes vers nos filières dont les débouchés sont variés mais méconnus du public.

De façon plus globale, les mathématiques fondamentales et appliquées ont un impact socio-économique très important en France. Celui-ci fait l'objet pour la première fois dans notre pays d'une étude commanditée par l'Agence pour les Mathématiques en Interaction avec l'Entreprise et la Société, en partenariat avec la Fondation Sciences Mathématiques de Paris et la Fondation Jacques Hadamard ; le rapport final sera publié le 27 mai prochain.

La SMF est consciente de l'importance d'une telle étude, sa journée annuelle 2015 en sera l'illustration, avec une table ronde sur le sujet et des exposés scientifiques axés sur les applications des mathématiques fondamentales.

Le 27 avril 2015

Marc PEIGNÉ, président de la SMF

La *Gazette* consacre un dossier aux Big Data, c'est-à-dire aux mégadonnées. Celles-ci affectent de façon grandissante de nombreux secteurs d'activité : la finance, la santé, l'e-commerce, la gestion des risques, et bien sûr la recherche scientifique. L'exploitation de gigantesques bases de données soulève de nouvelles questions à l'intersection des mathématiques et de l'informatique. Les enjeux économiques considérables conduisent à la création de nouveaux masters faisant intervenir les mathématiques. Pour mieux comprendre ce domaine, nous vous proposons trois articles complémentaires émanant des milieux de la recherche, d'une start-up, et d'un établissement financier.

Les mathématiques des Big Data

• É. Moulines

La taille des collections de données croît de manière exponentielle. Chaque jour, 2,5 quintillion d'octets de données sont créés. Plus de 90% des données disponibles aujourd'hui ont été créés au cours des deux dernières années. Ces données proviennent de sources très diverses, des *posts* dans des médias sociaux, des collections partagées de photographies, de vidéos, de musique, des traces de visites sur des sites web, des données de transactions sur des sites marchands, des objets connectés. Le Big Data a en quelques années pénétré de très nombreux domaines d'activités : santé, grande distribution, banque et assurance, politiques publiques, sécurité, mais aussi recherche scientifique. Ne trouve-t-on pas des applications du Big Data dans des domaines aussi variés que le calcul de *bid* sur des plateformes de ad-exchange, la recommandation de contenus, la détection d'effets secondaires d'association de molécules thérapeutiques, le *churning*, le climat, la génomique ?

Le « Big Data » (ou « méga-données » en français) recouvre l'ensemble des problématiques associées à la collecte et à l'exploitation de très grands ensembles de données, de types, formats, natures extrêmement variés (textes, nombres, clics, signaux capteurs, etc.). Je rajouterai que l'on est en face d'un problème « Big Data » lorsqu'il est impossible de traiter ces données au moyen d'algorithmes « état de l'art » sur des plateformes de calcul « traditionnelles ». Le Big Data a déjà un impact considérable dans de nombreux domaines. Les enjeux financiers sont saisissants et expliquent pourquoi la plupart des acteurs économiques considèrent le Big Data comme un axe fondamental de leur stratégie : McKinsey dans son rapport *Big Data, the next frontier for innovation, competition and productivity,* mentionne que le Big Data permettrait d'économiser chaque année 300 milliards d'USD aux politiques de santé aux USA, 250 milliards d'euros aux politiques publiques (plus que le produit intérieur brut de la Grèce), d'engendrer 600 milliards de dollars de consommation en utilisant les données de localisation des consommateurs, etc.

Pour parvenir à collecter puis à valoriser ces données, il est indispensable de développer de nouvelles architectures de stockage et de calcul réparti à très grande échelle, et de concevoir des méthodes innovantes de traitement pour en extraire

l'information disponible, que j'entends ici dans un sens très large que je tenterai de préciser dans la suite. Des avancées significatives ont été réalisées au cours de la dernière décennie, mais les besoins, sans cesse réévalués, sont encore très loin d'être tous satisfaits.

Le Big Data pose aux statisticiens des questions difficiles. Les corpus à analyser comportent un très grand nombre d'observations (souvent plusieurs milliards) ; chaque observation peut elle-même être dans certains cas de très grande dimension et les données qui la composent sont souvent produites par des sources d'information multiples et hétérogènes ; certaines données sont des flux « haute-fréquence » produits par des capteurs, d'autres des textes, des données collectées dans des cookies… Ces différentes caractéristiques, qui sont au cœur même du Big Data, engendrent des difficultés d'analyse : les approches statistiques « classiques » sont souvent inopérantes, ou alors trop coûteuses numériquement tant à cause du volume que de la variété des données.

De plus, contrairement aux statistiques « traditionnelles », les données sont collectées de manière « opportuniste » et non pas à travers un plan d'expérience, établi avant l'expérience et adapté à la tâche. Les biais d'échantillonnage sont donc extrêmement importants. La qualité de la collecte des données n'est pas contrôlée et est souvent médiocre : des données peuvent être manquantes, des erreurs d'étiquetage ont pu être commises, les capteurs ne sont pas calibrés de façon rigoureuse et produisent des données entâchées de forts niveaux de bruit. Les traitements statistiques doivent impérativement prendre en compte la médiocre qualité de la collecte et donc être robustes à ces sources de biais et de bruit.

Le très grand volume de données et la vitesse de traitement nécessitent de développer des méthodes numériques très sophistiquées. Effectuer une simple régression linéaire multiple peut poser des problèmes compliqués quand on cherche à analyser un milliard d'observations en dimension un million et que les données sont très largement réparties. Un certain nombre de méthodes et de techniques développées dans un monde où les ensembles de données étaient de taille limitée ont pu être adaptées avec succès au Big Data. Il s'agit toutefois d'exceptions : les problèmes de Big Data requièrent des solutions spécifiques, reposant sur des théories et des principes radicalement nouveaux. Les développements dans le domaine du Big Data associent l'informatique dans son ensemble (de l'intelligence artificielle aux bases de données en passant par le calcul distribué), les statistiques (et l'apprentissage statistique, que je prends ici comme une seule et même discipline), le traitement du signal et des images, l'optimisation (grand problème convexe, optimisation distribuée), les sciences humaines et sociales (sociologie, économie). Ceci signifie qu'une application Big Data requiert une approche trans-disciplinaire, et que les entreprises et les laboratoires engagés dans le Big Data doivent être d'un type nouveau, mettant côte-à-côte mathématiciens, informaticiens, économistes et sociologues (nous en sommes encore très loin dans le monde académique !). Ces développements méthodologiques et théoriques, ce qui est très original, proviennent aussi bien du monde académique que des entreprises (des start-up aux géants du web). Ce sont souvent les entreprises qui sont les moteurs de la recherche (et qui créent un *brain drain* considérable dans les laboratoires, les salaires proposés par Google, Facebook et Criteo faisant évidemment tourner les têtes…).

Dans ce court article, je me focaliserai essentiellement sur les challenges statistiques que me semble poser le Big Data. En se référant au très complet *Oxford Dictionary of statistical terms* (OUP, 2006), le domaine des statistiques est « l'étude de la collecte, de l'analyse, de l'interprétation, de la présentation et de l'organisation des données ». On se doute aisément que les statistiques sont au cœur des problématiques du Big Data !

1. Le Big Data en quelques mots

La numérisation de nos sociétés est exponentielle. Tous nos déplacements sont connus et *Google Now* est capable de me dire lorsque je sors de mon bureau combien de temps je vais mettre pour rejoindre mon domicile si je prends un vélib ou si je prends le métro. Dès que mon téléphone portable est allumé, les différentes stations de base que reçoivent mon portable sont instantanément connues par l'opérateur de réseau ; si mon GPS est ouvert, ma position est connue avec une précision de quelques mètres à l'échelle du globe. Tout ce que je fais, les personnes que je rencontre, mes loisirs sont disponibles sur Facebook (là, j'exagère un peu, ma page Facebook n'est pas très active !) Vous pouvez connaître mes goûts cinématographiques, mes coups de cœur pour tel ou tel spectacle, mes découvertes gastronomiques en consultant les réseaux

où je dépose régulièrement des informations, des photos, … Je ne vais d'ailleurs plus au restaurant ou dans un hôtel sans consulter La Fourchette ou TripAdvisor, qui me permettent de juger de la réputation des établissements. Toutes mes dépenses de santé, les traitements que je prends, mes consultations médicales sont tracées et analysées. Amazon m'écrit pour me suggérer l'achat de livres et je suis harcelé par la publicité ciblée dès que je navigue sur Internet.

Bien entendu, tout ce qui a été écrit depuis les premières heures de l'humanité est disponible en ligne, est numérisé, indexé… Nul besoin de vous déplacer dans une bibliothèque, toute la connaissance littéraire, scientifique, philosophique est disponible là, aux bouts de vos doigts. Picasa, Dropbox permettent de partager vos albums photographiques, Youtube et Dailymotion vos vidéos préférées…

Ceci est la partie « émergée » de l'iceberg numérique, l'information que nous avons plus ou moins conscience de partager ou les traces que nous acceptons de laisser. Il y a une face plus obscure : notre monde est rempli de capteurs de toute nature, qui engendrent des données en grand nombre et souvent à très haute fréquence. Ces capteurs sont dans nos smartphones, dans nos automobiles (l'électronique embarquée représente plus de 40% du prix d'achat !) ; ils envahiront demain notre quotidien par l'intermédiaire des objets connectés dont le nombre explose lui aussi de façon exponentielle.

Les deux exemples que je vais développer sont un échantillon infime des applications, qui n'ont d'autres prétentions que de donner quelques ordres de grandeur. On pourrait multiplier de tels exemples.

2. Big Data pour le commerce et la finance

Le Big Data a investi depuis une dizaine d'années le commerce de détail. Aujourd'hui, toutes les transactions que vous effectuez sont enregistrées et le détail de vos achats est donc connu et analysé. On pourra bientôt vous dire lorsque vous passez en caisse que vous avez oublié d'acheter le sel. La quantité de données collectées par les applications de commerce (à l'échelle mondiale) double tous les 16 mois. Pour fixer les idées, chaque jour Wal-Mart enregistre 267 millions de transactions dans ses 6 000 points de vente. Pour collecter l'ensemble de ces transactions, Wal-Mart a développé un entrepôt de données de 4 petaoctets, c'est-à-dire 4.10^{15} octets (!) qui enregistre le détail de vos achats (identifié par votre carte de paiement ou votre carte de fidélité). En exploitant cette masse considérable d'informations à l'aide de méthodes de statistiques, Wal-Mart a développé de nouvelles stratégies de détermination des prix de vente et des campagnes publicitaires ciblées et personnalisées allant bien au-delà de la traditionnelle application à la gestion prédictive des stocks.

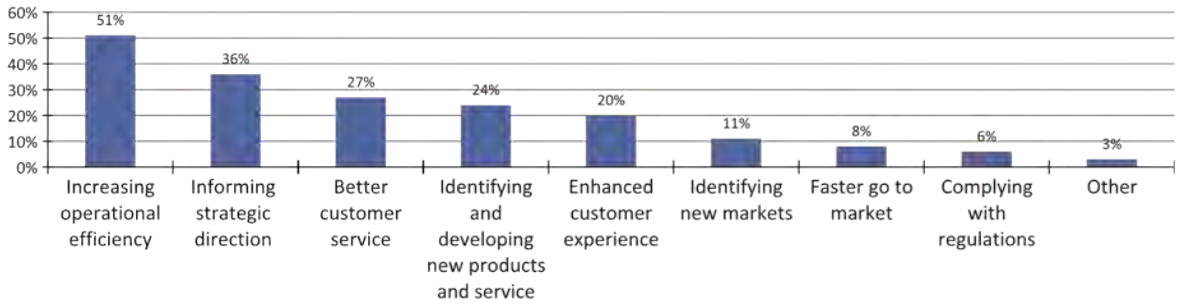
Les institutions financières disposent aujourd'hui de très nombreuses sources d'information, incluant le prix des actifs financiers, les taux de change des devises, les prix de très nombreux actifs contingents (options, futures), mais aussi des *news* financières, des analyses financières produites par des experts des différents marchés, et les données des réseaux sociaux qui permettent d'évaluer les « sentiments » sur le marché… Les fonds quantitatifs exploitent aujourd'hui l'ensemble de ces données pour élaborer des stratégies de gestion de portefeuille, s'appuyant non seulement sur des méthodes reposant sur des historiques de prix des actifs financiers mais aussi pour capter, en utilisant les posts sur les médias sociaux, le sentiment des opérateurs économiques. Au cours de la dernière décennie, de plus en plus de sociétés ont adopté des approches reposant sur de très vastes collections de données pour optimiser leur stratégie de fixation de prix, proposer des offres plus « personnalisées », réduire les risques et augmenter globalement leur productivité. Ces sociétés mettent en œuvre des solutions Big Data pour collecter, stocker, et analyser les données collectées de sources variées pour identifier les informations pertinentes permettant d'optimiser l'efficacité opérationnelle, de guider la prise de décision stratégique, d'identifier et de développer de nouveaux services et produits, d'identifier de nouveaux marchés, etc.

3. Big Data en recherche scientifique

Beaucoup de domaines scientifiques sont d'ores et déjà fortement impactés par le BigData. Par exemple, l'astronomie, la météorologie, la génomique sont des sciences collectant des nombres impressionnants de données et les exploitant pour faire avancer l'état de la connaissance.

Ainsi, un télescope peut être vu comme une caméra numérique de très grande. Un téléscope fournit une quantité considérable d'images. Par

Figure 1 – D'après Gartner, 2014. L'ordonnée indique le pourcentage d'entreprises qui pensent que le Big Data peut les aider à répondre à des questions particulières. Plus de 50% des 560 entreprises sondées pensent que le Big Data peut les aider à améliorer leur efficacité opérationnelle.



exemple, le *Large Synoptic Survey Telescope* (LSST) enregistre 30 trillions d'octets d'images chaque jour. Le LSST va donc engendrer chaque jour deux fois plus d'informations que le SLOAN digital survey (le téléscope de génération précédente) pendant toute son existence ! Les astronomes vont tenter, à l'aide de données, de s'approcher toujours plus près de la résolution de la fascinante énigme que constitue la création de notre univers.

Le *Large Hadron Collider (LHC)* quant à lui est un accélérateur de particules qui engendre 60 téraoctets de données chaque jour. Ces données sont susceptibles de confirmer ou d'infirmer les théories dont nous disposons sur la physique des hautes énergies gouvernant la structure de la matière.

Le *discovery supercomputing cluster* du *NASA Center for Climate Simulation* (NCCS) stocke 32 pétaoctets d'observations sur le climat et de résultats de simulation de modèles climatiques. Ces données jouent un rôle essentiel pour étudier les différents scénarios d'évolution de nos climats et l'impact des politiques publiques de réduction de gaz à effets de serre.

De nombreux autres projets de *e-Sciences* sont en gestation dans de très nombreux domaines de la connaissance : environnement, climat, géologie, biologie, et sociologie. Un point commun de toutes ces approches est la collecte d'ensembles très importants de données qui nécessitent des méthodes d'analyse automatiques.

4. Les difficultés

Mettre en œuvre des applications Big Data ne va bien entendu pas sans soulever des difficultés majeures. Ces difficultés concernent aussi bien la collecte, que le stockage, la recherche, l'indexation, l'analyse, ou la visualisation de ces ensembles de données.

Si, comme nous l'avons vu, la quantité d'information produite et stockée augmente de façon exponentielle, la capacité de traitement de ces informations n'a pas cru à un tel rythme. Dans de nombreuses applications Big Data, les techniques de l'« état de l'art » s'avèrent insuffisantes pour résoudre de façon satisfaisante le problème posé ; en particulier, on est encore loin de savoir exploiter en « temps réel » les informations disponibles.

Penchons-nous sur la première difficulté de taille dans la construction d'un système Big Data à savoir la collecte et l'archivage de très grands ensembles de données. La variété et le volume considérable des données collectées requièrent de définir des méthodes permettant de stocker et d'indexer des données non structurées ou semi-structurées, en vue de leur analyse. Ce problème a suscité un très grand nombre de travaux et de développements en informatique. Les architectures de stockage Big Data reposent sur différentes implémentations d'un concept de base, appelé « NoSQL » (Not Only SQL). De façon très schématique, NoSQL utilise certains mécanismes de base de données relationnelles, mais ne retient que les mécanismes de requêtes qui peuvent être implémentés de façon rapide.

La deuxième difficulté provient de la qualité de la collecte des données qui dans de nombreux cas n'est pas rigoureusement contrôlée : pas de plan d'expériences, pas de données soigneusement recoupées et identifiées, pas de stratification précise des échantillons, pas de détection de données aberrantes… Du coup, les algorithmes de Big Data doivent s'accommoder de données de qualité mé-

diocre. Les données Big Data sont souvent incomplètes, entachées d'erreurs, ou de bruit, pour parler la langue d'un traiteur du signal (mais les sources de bruit en traitement de signal sont le plus souvent beaucoup plus faciles à identifier et du coup à combattre).

Avant d'être archivées et analysées ces données doivent être « pré-traitées », « filtrées »... Ce processus est appelé en anglais *data curation*. Je ne suis pas sûr de connaître une excellente traduction française, disons « conditionnement des données ». Le processus de *data curation* recouvre de nombreuses étapes de consolidation des sources, réorganisation de l'architecture d'accès aux données pour en faciliter l'accès, d'identification des biais de collecte, de recherche de données aberrantes, de recodage, etc. Cette étape, en amont de l'analyse, est absolument indispensable. Elle ne repose pas sur de « grands principes » théoriques mais requiert une sérieuse dose d'expertise, de bon sens et surtout, beaucoup de patience.

Après la *Data Curation* vient typiquement l'analyse. Les tâches que l'on peut assigner à un système de traitement Big Data se séparent en deux groupes : les tâches « prédictives » ou « décisionnelles » et les tâches de « découverte » ou de « minage » des données. Ces deux grandes classes de problèmes ont des objectifs et des contraintes très différents.

Les tâches prédictives recouvrent en particulier la *classification* et la *prédiction*, mais ne se limitent pas à ces problèmes. La classification est un ensemble de méthodes qui permettent d'identifier la « classe » d'une donnée, en utilisant une base de données d'apprentissage préalablement étiquetées. La prédiction (ou régression) est un ensemble de méthodes statistiques permettant, en utilisant un ensemble d'apprentissage, une réponse en fonction d'un ensemble de variables explicatives. Cette réponse peut être un label catégoriel, attribut numérique, voire une fonction (pour la régression fonctionnelle) etc. Les tâches prédictives ont dans certains cas une dimension « temps réel » (pour fixer un prix, identifier un morceau de musique sur le web,...).

Les tâches de « découverte » ou de « minage » (*data mining*) consistent à extraire des « structures » de grands ensembles de données. Ces structures peuvent être des *clusters* (des groupes d'observations ayant des comportements homogènes), des règles d'association (pour détecter des relations entre ensembles de variables), de l'analyse de réseaux (identifier les relations entre les différents nœuds d'un réseau), de l'analyse de sentiments (pour extraire une information subjective d'un ensemble de textes). Ces tâches de *data mining* font plutôt l'objet d'analyses « hors-ligne ».

La dichotomie entre méthodes prédictives et *data mining* est assez floue. Par exemple, les systèmes de *recommandation*, qui visent à présenter à un utilisateur des éléments d'information (films, musique, livres, news, images, pages Web, etc.) qui sont susceptibles de l'intéresser, associent des méthodes prédictives et de *data mining*.

Mettre en œuvre une application de classification, de régression ou de *data mining* dans un cadre Big Data pose bien entendu des questions spécifiques difficiles.

Le premier obstacle à franchir est l'hétérogénéité. Les données Big Data sont souvent obtenues en agrégeant différentes sources de données de nature très différentes. On peut être amené à traiter de façon simultanée des données numériques, catégorielles, mais aussi textuelles, des données de préférence, des historiques de navigation, des historiques d'achat sur des sites de e-commerce... Des données de médias sociaux, analysées à l'aide de méthodes de traitements de langue naturelle, peuvent être fusionnées avec des données de vente pour déterminer l'effet d'une campagne publicitaire sur le sentiment des consommateurs sur un produit et les comportements d'achat. La pollution à Paris est surveillée en temps réel en assimilant des observations de capteurs mesurant la concentration de polluant et de particules, de données climatiques (flux solaire, températures, vitesses et orientation du vent), de capteurs de trafic dédiés, de systèmes de vidéosurveillance. La capacité d'extraire des informations pertinentes des données obtenues en agrégeant des sources de nature très différentes en les fusionnant est à coup sûr une des clefs du succès des systèmes Big Data.

Le développement d'un algorithme d'agrégation et de fusion nécessite une première étape de « recodage », permettant de représenter cette information sous une forme exploitable par un algorithme de traitement. Il est souvent difficile de mélanger dans une même analyse des données catégorielles et numériques... on imagine sans peine qu'il est encore plus difficile d'agréger des données numériques, des textes, des données de recommandation... Cette étape de définition d'une « bonne représentation » est très délicate et constitue un véritable défi scientifique.

Dans de nombreuses applications, la tendance est d'enregistrer le maximum d'informations possibles et de laisser les méthodes de classification, de régression et de data mining de faire le « tri » entre l'information utile (pour la tâche considérée) de l'information superflue. Quelle que soit la tâche considérée et la méthode utilisée, travailler avec un grand nombre de « variables explicatives » va impliquer d'estimer et de tester de très nombreux paramètres. Il est bien connu que les erreurs d'estimation et de tests se composent. Dans un modèle de régression linéaire, même dans la situation la plus favorable où la matrice de régression est orthogonale, la variance des estimateurs croît linéairement avec le nombre de paramètres : cette augmentation de la variance peut devenir rapidement gênante même si le nombre d'observations est très grand.

5. Quelques exemples de recherches en Big Data

Le Big Data met en jeu un grand nombre de domaines des mathématiques appliquées : statistiques au sens large, traitement du signal et des images, optimisation convexe et non convexe, probabilités appliquées (graphes aléatoires, algorithmes stochastiques…). La recherche dans le monde du Big Data est un monde dont il est encore difficile de cerner les contours. D'une part, les bases algorithmiques et statistiques de techniques aussi élémentaires que la régression linéaire multiples, la régression logistique, l'analyse de la variance ou l'analyse en composantes principales doivent être complètement modifiées pour pouvoir passer à l'échelle. D'autre part, le Big Data est une source quasi-infinie de nouveaux problèmes, qui requièrent à la fois de développer de nouvelles théories et des méthodes numériques innovantes.

Pour donner une idée très fragmentaire du type de recherche, je vais décrire très succinctement des travaux que j'ai menés récemment. Il s'agit de prédire une réponse (dans mon cas un label de classes), à partir d'un grand ensemble de données d'expressions de gènes, sur une grande population. Le nombre de variables explicatives est ici de quelques milliers, mais l'observation est incomplète : des régresseurs sont manquants et doivent donc être simulés (en statistique, de tels modèles sont appelés à *effet mixte*).

Une première approche consiste à construire une représentation compressée des variables explicatives en préservant l'information disponible. Ceci revient à construire une fonction définie sur l'espace des variables explicatives dans un espace (ou une variété pour les méthodes non-linéaires) de dimension beaucoup plus faible en tentant de minimiser la perte d'information. Il existe un grand nombre de méthodes pour accomplir une telle tâche. L'analyse en composante principale, qui revient à projeter les observations orthogonalement sur les espaces dominants de la matrice de covariance empirique (les espaces propres associés aux plus grandes valeurs propres, la dimension de l'espace de projection dépendant de la réduction de dimension souhaitée) est sûrement la méthode la plus couramment utilisée. Estimer l'espace dominant d'une matrice de covariance (qui revient à calculer les vecteurs singuliers « à gauche » de la matrice des observations) en très grande dimension est un problème redoutablement difficile numériquement. Les méthodes non-linéaires, comme les méthodes d'ACP à noyaux, des méthodes d'apprentissage de variétés comme ISOMAP ou « *locally linear embedding* » ou « *Laplacian eigenmaps* », sont encore plus délicates à mettre en œuvre.

Une seconde approche consiste à sélectionner les variables explicatives pertinentes pour travailler avec des modèles « parcimonieux ». Les modèles « parcimonieux » sont la déclinaison aux statistiques du principe du « rasoir d'Ockham » *Entia non sunt multiplicanda praeter necessitatem*, littéralement « les entités ne doivent pas être multipliées par delà ce qui est nécessaire » (source Wikipédia). La formalisation mathématique du rasoir d'Ockham est la base de la théorie de l'apprentissage, dont les principes (théorie de la décision) remontent aux fondations même des statistiques mathématiques, au début du xx^{e} siècle et qui s'est considérablement développée dès la fin des années 1970.

L'approche classique suggère de choisir les variables en minimisant sur la collection de tous les modèles le risque empirique (le plus souvent, une vraisemblance ou quasi-vraisemblance) pénalisé par une fonction mesurant la complexité du modèle qui peut être interprétée comme une distribution sur la collection des modèles. L'exemple le plus simple de mesure de complexité est le nombre de variables sélectionnées mais des formes plus subtiles de complexité doivent être utilisées lorsque le nombre de modèles possibles est grand devant le nombre d'observations. Lorsque la pénalité est bien « calibrée », il est possible d'établir des inégalités « oracles » qui permettent de comparer le risque de la procé-

dure de décision obtenue en minimisant le risque empirique pénalisé et une procédure de décision à qui un « oracle » aurait donné les variables pertinentes. Cette approche a été développée dans le courant des années 1990-2000 en partant d'inégalités non asymptotiques. Des résultats très fins sont aujourd'hui disponibles pour une grande classe de modèles.

La difficulté avec ce genre d'approches est que la minimisation du risque empirique pénalisé est un problème combinatoire, dont la complexité est rédhibitoire lorsque le nombre de variables explicatives dépasse quelques dizaines !

Pour contourner cette difficulté, de nombreux auteurs ont proposé d'utiliser des pénalités de complexité dont l'optimisation ne requiert pas de recherche exhaustive. Les recherches se sont tout d'abord concentrées sur les pénalités convexes. L'exemple le plus emblématique est la pénalité LASSO (*Least-Absolute Shrinkage and Selection Operator*, la norme L1 des coefficients du prédicteur ; cette pénalité a été le point de départ d'un ensemble très fructueux de recherche, donnant naissance à une grande variété de pénalités, qui permettent de « traduire » des connaissances a priori sur le modèle (group-LASSO, fused LASSO)… Des pénalités non convexes comme SCAD (*smoothly clipped absolute deviation*) sont aujourd'hui proposées et analysées.

Même lorsque les critères sont « calculables », le nombre d'observations et leur dimension nécessitent de repenser fondamentalement les algorithmes de calcul. Les données de *Genome_wide association study comportent* aujourd'hui des centaines de milliers d'individus, ce qui rend difficile le même calcul du risque empirique et a fortiori du gradient du risque, surtout lorsque le nombre de variables explicatives peut atteindre des dizaines de milliers.

La résolution de problèmes de grande dimension est non seulement très coûteuse en temps calcul, mais elle est difficile numériquement. La robustesse des algorithmes est donc une condition essentielle à leur mise en œuvre. Pour illustrer ces difficultés supposons que le risque est convexe régulier (disons continûment différentiable, de gradient Lipshitzien) et que la pénalité est convexe, mais non différentiable (ce qui est le cas de toutes les pénalités favorisant les solutions parcimonieuses). En grande dimension, seule les méthodes de premier ordre (utilisant le gradient de la fonction ou le sous-gradient) peuvent être mises en œuvre. La méthode la plus élémentaire pour résoudre ce problème est l'algorithme de « descente du sous-gradient ». Comme je l'ai souligné plus haut, pour de très grands ensembles de données, des opérations aussi élémentaires que de calculer la valeur d'une fonction ou de son gradient peuvent s'avérer impossibles à mettre en œuvre. Il peut s'avérer plus approprié de mettre à jour seulement un sous-ensemble des paramètres, voire de ne mettre à jour qu'un paramètre (on parle alors d'algorithme de « descente de coordonnées »). Dans ce dernier cas, la mise à jour peut être explicite (on résout « explicitement » le problème d'optimisation à une dimension), et ces résolutions peuvent être alors très largement parallélisées.

Une autre approche (plus efficace dans certains problèmes) consiste à utiliser un algorithme de gradient pour la partie régulière (risque) et des méthodes proximales pour la partie non-régulière. Il est aussi possible de ne travailler que sur des sous-ensembles des observations (au lieu de calculer le gradient sur l'ensemble des données, on extrait de l'ensemble des données un sous-échantillon, de façon aléatoire ou déterministe, et on n'évalue le gradient que sur ce sous-échantillon). On obtient de la sorte des algorithmes de gradients stochastiques « proximaux » dont l'exemple emblématique est le gradient stochastique « seuillé ».

Un des challenges actuels consiste à étendre ces méthodes à des pénalités non convexes, comme SCAD. Bien entendu, il est impossible d'obtenir un minimum global dans un tel contexte (les heuristiques d'optimisation globale ne sont pas du tout appropriées pour de telles dimensions). La seule approche possible est de proposer une heuristique d'optimisation (souvent fortement inspirée du cas convexe), puis de caractériser finement les points stationnaires de ces heuristiques. Une telle approche a été menée pour la pénalité SCAD. On cherche tout d'abord un minimum pour une pénalité de type LASSO puis on cherche dans un voisinage de cette solution la solution du problème pénalisé par SCAD. Bien que cet algorithme ne converge pas globalement, on peut montrer que la solution « locale » ainsi trouvée satisfait à la même inégalité oracle que l'estimateur « global ». L'idée d'étudier les propriétés statistiques d'estimateurs qui ne sont pas des optimums globaux de critères mais des points stationnaires d'heuristiques d'optimisation (et qui sont donc des estimateurs « calculables ») est une direction de recherche importante des statistiques « numériques ».

6. Conclusion

Le Big Data est un domaine très actif tant en recherche que dans le monde économique. Les besoins de formation sont très importants. Le Big Data est considéré par beaucoup d'entreprises comme un des éléments clefs de leur compétitivité. S'il est difficile de faire des projections dans ce domaine, ce champ majeur de création de richesses nécessitera tout d'abord des spécialistes de l'analyse des données qui devront allier des compétences mathématiques de pointe et de l'informatique (associant algorithmique numérique, bases de données et calculs répartis). Aux États-Unis, les besoins pour ce type de profils représentaient 150 000 postes en 2008, et devraient atteindre 425 000 à 475 000 postes en 2018 (d'après une étude McKinsey). Au-delà de ces profils hautement spécialisés, nombre de managers devront maîtriser ces sujets et disposer des compétences statistiques nécessaires pour interpréter les données et les exploiter à des fins opérationnelles ou commerciales : si l'on prend à nouveau l'exemple des États-Unis, ce type de postes de managers familiers des Big Data devrait concerner 4 millions de personnes en 2018. Les mathématiciens ont une belle carte à jouer pour répondre à ces besoins !

Éric Moulines
Éric Moulines anime une équipe de traitement statistique au sein du LCTI de Télécom ParisTech, où il est professeur depuis 1996. Il a reçu la médaille d'argent du CNRS en 2010.

Portrait de David Bessis, créateur de start-up

Propos recueillis par G. Octavia assistée de A. Jacquet
Fondation Sciences Mathématiques de Paris

Il s'agit dune retranscription d'une interview effectuée en 2013 dont la source se trouve à l'adresse suivante : `http://www.sciencesmaths-paris.fr/fr/laventurier-du-big-data-502.htm`

Il y a deux moments dans le parcours professionnel de David Bessis. Une première carrière de mathématicien, puis la création d'une start-up, *tinyclues*, qui marque les débuts d'une carrière d'entrepreneur. Si ses travaux de chercheur sont très éloignés du domaine d'expertise de *tinyclues*, David Bessis revendique cependant une certaine continuité dans sa trajectoire : « Passer du monde académique au monde de l'entreprise est une transition rare mais naturelle. Le chercheur et l'entrepreneur partagent les mêmes qualités : la créativité, le courage et la persévérance ».

Son itinéraire est cependant encore atypique. Après avoir soutenu sa thèse, résolument axée sur les mathématiques fondamentales, il entre au CNRS et y reste sept ans. Son habilitation obtenue, il a cependant l'impression de clore un chapitre : « Je voulais trouver un autre chantier auquel m'atteler. » Son parcours prend alors une nouvelle tournure. Il se met en disponibilité hors du CNRS et se lance dans le conseil en entreprise. Plus précisément, c'est au sein d'une agence de marketing digital qu'il officie. Il se familiarise avec les technologies utilisées et contribue à leur développement. Les mathématiques à l'œuvre sont pourtant nouvelles pour lui.

Après un an dans cette première entreprise, il ressent l'envie de fonder sa propre start-up. Une démarche là encore naturelle à ses yeux : « La création est inhérente à l'activité du chercheur ». En 2010, il crée donc, avec un associé, *tinyclues*, spécialisée dans le Big Data, c'est-à-dire dans l'extraction et l'analyse d'un très grand nombre de données. Pendant plusieurs mois, il établit les prototypes des

logiciels de *data mining* nécessaires au fonctionnement de la start-up. Tout s'accélère alors : en avril 2011 les premiers salariés arrivent et les premiers contrats se font. En particulier, *tinyclues* est sollicitée par des sites marchands. L'enjeu est alors de pouvoir définir le plus précisément possible le profil des consommateurs, utilisé ensuite à des fins marketing.

Aujourd'hui, *tinyclues* emploie 10 personnes. Des développeurs de logiciels, mais aussi des spécialistes du *data mining*. Les mathématiciens y ont toute leur place.

Comment avez-vous bifurqué vers le monde de l'entreprise ?

J'ai eu une première carrière de chercheur en mathématiques pures et réalisé une thèse alliant algèbre, géométrie, topologie, sur les groupes de réflexions et les groupes de tresses.

J'ai fait de la recherche pendant plusieurs années avec la certitude que je serais déconnecté de la réalité économique pendant la totalité de ma vie. En 2006, j'ai fini la rédaction d'un gros théorème – gros pour moi, pas pour l'histoire des mathématiques – un peu lessivé. J'ai soutenu mon habilitation dans la foulée. Il s'était écoulé une douzaine d'années depuis le moment où j'avais commencé à me lancer dans le monde de la recherche. J'étais arrivé au bout des problématiques sur lesquelles je m'étais lancé. Il me fallait trouver un autre gros chantier.

C'est alors que je le recherchais que je me suis laissé attirer par autre chose. Par curiosité, j'ai décidé de passer de temps en temps une journée en entreprise. Je me suis retrouvé en contact avec une entreprise qui faisait du marketing digital.

Je me suis ensuite mis en disponibilité pour travailler dans cette entreprise, trois mois plus tard, j'en dirigeais la R&D, et j'y ai passé à peu près un an.

J'ai découvert le fait de travailler avec des gens au quotidien. J'ai découvert des domaines où tout était à inventer, où l'on pouvait réellement changer les choses très vite et très simplement. Je me suis lancé dans l'aventure. Mon entrée dans le monde de l'entreprise s'est faite en travaillant dans le marketing digital.

C'était à une époque où il y avait un basculement dans les problématiques du marketing digital. Dans ce domaine, il y une partie qui concerne le *display* au sens général, c'est-à-dire tout ce qui concerne les éléments visuels (bandeaux, bannières, etc.), et une partie qui est le *Push* ou le CRM (*Customer relation ship management*), c'est-à-dire le fait de contacter quelqu'un. Quand vous contactez quelqu'un pour lui proposer un produit, le plus probable est que cela ne l'intéresse pas. Le risque alors, c'est qu'il manifeste son non-intérêt soit en se désabonnant, soit en disant que ceci est du spam. Or si trop de gens disent que ceci est du spam, cela devient du spam.

Les gens qui gèrent les adresses mail (gmail, hotmail, etc.) vont alors complètement censurer la communication. Donc la problématique de l'entreprise où je travaillais à ce moment-là, c'était de trouver de bonnes méthodes pour que les messages qui étaient envoyés soient plus intéressants pour les gens qui allaient les recevoir. J'ai donc travaillé sur la mise en place d'outils qui permettaient de manière prédictive d'améliorer cet intérêt.

Et les mathématiques dans tout cela ?

J'ai découvert en travaillant sur ces sujets qu'il y avait un certain nombre d'outils qui existaient, des logiciels dits de *data mining*, de fouille de données. Le *data mining* est l'ensemble des procédés qui permettent de manipuler des données pour prédire des choses, pour détecter des *patterns*. Je ne connaissais pas du tout cette branche des mathématiques : elle mobilise des statistiques, or j'avais fait des mathématiques très algébriques. En entreprise, les savoirs s'acquièrent très rapidement. D'autant plus rapidement pour un mathématicien, curieux de nature et qui tire là le bénéfice de sa formation. J'ai appris, et mon intuition mathématique, même si je n'avais pas étudié ce sujet, m'a fait comprendre que les outils utilisés ne marchaient pas très bien. C'est là que j'ai découvert ce sujet qui s'appelle aujourd'hui le Big Data.

À l'époque il n'y avait pas de nom pour cela. Vous avez des masses de données gigantesques, vous avez des milliards d'événements qui concernent des millions de gens, et vous vous dites que dans cette masse d'informations, il y a des choses à prévoir. Toute la difficulté réside dans le fait que vous ne pouvez pas prévoir de façon directe, parce que les signaux sont de très très basse fréquence. Si vous avez écrit *naruto*[1] dans votre adresse mail, vous avez plus de chances d'acheter des mangas. Par contre, si vous cherchez la corrélation de façon directe, vous ne la trouverez pas, parce que

1. Il s'agit du nom d'un titre de manga.

vous avez peut-être vendu 200 mangas, et qu'il y a 30 personnes en France qui ont *naruto* dans leur adresse mail. Vous ne pouvez pas, de façon directe, mettre en relation, une chose que vous voulez prédire avec un prédicteur.

Il y a eu depuis une dizaine d'années des techniques mathématiques qui viennent de nombreux domaines d'application, notamment en génétique. Dans ce domaine, le problème est le suivant : vous ne disposez du génome que de quelques personnes ; or le génome est très très long ; vous avez quelques cas d'études, et vous connaissez quelques pathologies, quelques caractéristiques morphologiques, et vous voulez chercher des corrélations. Si vous les cherchez de façon directe, cela ne va pas fonctionner. Vous allez donc essayer de consolider le signal, en cherchant à un niveau abstrait des concepts. Si vous avez un graphe social, des millions de gens, des milliers de produits, qui a acheté quoi, qui suit telle personne sur Twitter, etc., vous pouvez utiliser la géométrie de ce graphe pour consolider les données. Une fois que vous avez consolidé les données, vous pouvez faire les corrélations. Vous fabriquez la sémantique abstraite à partir de la structure globale d'une masse considérable de données.

À quoi cela s'applique-t-il concrètement ?

La question des domaines d'application est une question très intéressante. Parce que quand on fait des mathématiques, on se dit toujours que cela peut potentiellement s'appliquer. Quand on crée une entreprise, on veut que cela s'applique réellement. Et le chemin vers l'application recèle plein de difficultés, des difficultés de situation de marché, réglementaires, des difficultés d'acceptation de la technologie par les acteurs du secteur. Aujourd'hui, l'entreprise que j'ai créée a pour domaine d'application principal le marketing. C'est un domaine où il y a des entreprises qui sont prêtes à investir dans la technologie, à investir dans les choses qu'elles ne connaissent pas bien. Elles ont un goût pour la prise de risque. Mais c'est aussi un domaine où si vous faites une erreur, vous ne tuez pas des millions de gens, c'est un domaine d'application très simple en fait. On est capable pour nos clients qui sont des grands acteurs du marketing digital, comme *PriceMinister* par exemple, de leur permettre de réduire de façon très substantielle le nombre de mails qu'ils vont envoyer, de diviser par un facteur de l'ordre de 2 à 3 le nombre de désabonnements qu'ils vont engendrer. Les technologies qui sont derrière cette application que nous commercialisons peuvent servir à beaucoup d'autres choses. En matière de santé par exemple, l'ensemble des prescriptions médicales enregistrées par l'assurance maladie, les feuilles de soin, ressemble beaucoup à l'ensemble des transactions réalisées par un gros e-commerçant. Quand dans votre panier de médicaments, il y a tel et tel médicament, on suppose que vous avez telle maladie. Mais ce qui est intéressant avec ces techniques, c'est qu'on peut faire émerger des *patterns* qui n'étaient pas verbalisés. On peut se rendre compte qu'il existe des catégories de diagnostics qui sont transverses. On peut peut-être ainsi détecter des maladies qui n'ont pas encore de noms. Cela a été le cas du sida qui a été découvert par des analystes de services de santé américains. Le genre de technologie que l'on déploie dans le cadre du e-commerce permet clairement de détecter ce genre de choses.

Comment s'est opérée pour vous la transition entre le monde académique et la création de *tiny-clues* ?

Quand on est chercheur, on est dans une problématique de création. C'est très dur d'accepter, dans la durée, de travailler dans une structure qui va vous dire ce que vous devez faire. J'avais eu l'habitude d'avoir une totale liberté dans le choix de mes thèmes de recherche, et à mon sens ma vraie valeur ajoutée était la création. Cependant j'avais aussi l'impression que je comprenais des choses sur les problématiques de Big Data, de *data mining*, qui n'étaient pas comprises par la majorité des gens. La transition m'a donc paru assez naturelle. L'entreprise a été créée au printemps 2010. Je l'ai montée avec un associé qui à l'époque avait un autre travail. Pendant une dizaine de mois, avant et après la création de l'entreprise, j'étais seul derrière mon ordinateur en train d'essayer de prototyper les algorithmes et une architecture logicielle qui étaient le squelette de ce qu'est devenue la plateforme technologique que l'on a aujourd'hui. Au bout de quelques mois, mon associé a quitté le travail qu'il avait pour me rejoindre.

Nous nous sommes lancés, les premiers salariés à plein temps sont arrivés en avril 2011.

Avez-vous rencontré des difficultés au départ en tant qu'entrepreneur ?

Ce qui est dur dans notre secteur, c'est que l'on travaille sur des données qui sont celles de nos clients, on ne collecte pas nous-mêmes les données qui sont très réglementées par la CNIL. Pour tester nos algorithmes, il fallait que l'on ait accès à des

données. Nous sommes donc allés voir des entreprises et leur avons demandé de nous confier leurs données de façon très encadrée par un contrat, en leur proposant de les aider à résoudre les problèmes qui se posaient à elles. Nous étions en train de vendre quelque chose que nous savions faire sur le papier, mais que nous n'avions pas encore fait réellement. Cette période a duré 18 mois où l'on devait inventer en temps réel. C'est un peu comme si vous deviez traverser l'Atlantique sur un bateau que vous êtes en train de construire. Il y a quelque chose qui relève de l'aventure, et qui est particulièrement stimulant. Il y a cette phase qui est forcément un peu souterraine, où l'on ne peut pas avoir beaucoup de clients, car chaque client mobilise les ressources intellectuelles et pose des abîmes de réflexion et de doute.

Le but est de sortir de cela en ayant compris quels sont les vrais problèmes de nos clients et comment les résoudre. Aujourd'hui on rentre dans une phase, depuis le début de l'année 2013, où l'on a des produits standardisés. On peut aller voir des entreprises en leur disant que l'on peut résoudre tel problème, avec tel temps, tel coût et tel gain de performances.

Comment est composée l'équipe ?

Il y a une grosse équipe importante de développement logiciel. L'informatique pose d'ailleurs des problèmes intellectuels et conceptuels qui ressemblent à ceux que posent les mathématiques, les mathématiques d'il y a 100 ans quand il y avait Hilbert et ses problématisations de ce que devaient être les mathématiques. Il y a quelque chose qui a la même saveur en informatique. On a une équipe qui est plus *Data*, composée de statisticiens, d'informaticiens. On a aussi quelques postes plus orientés sur les opérations clients ou sur le marketing, et il y a des mathématiciens.

Je pense que la formation est importante mais l'expérience de chercheur l'est encore plus. Ce que l'on apprend, quand on fait de la recherche, c'est à se confronter à des problèmes difficiles, à savoir quand on a une idée que les autres n'ont pas, et à porter cette idée des mois ou des années.

Ce que fait *tinyclues* aujourd'hui s'appuie sur des intuitions technologiques qui n'étaient pas des intuitions standard quand on a créé l'entreprise. Avoir le sang-froid intellectuel pour savoir qu'il y a des idées qui ne sont pas les idées standard, mais qui peuvent fonctionner, et qu'il va falloir du temps pour les porter à un stade de maturité, c'est typiquement de la problématique de recherche. Je ne vois pas de différence épistémologique entre la problématique de création d'entreprise et la problématique de recherche scientifique.

Il y a des différences de modes de travail, il y a beaucoup plus de pression, il y a des problèmes humains, matériels, pressants et stimulants, mais le fond de la création, c'est la même chose.

Comment aborder la transition entre le monde académique et le monde de l'entreprise ?

Je crois que c'est un peu une légende de dire que les entreprises sont fermées aux profils académiques. La vraie valeur ajoutée d'un mathématicien, c'est la créativité.

Plus que les connaissances purement académiques, c'est la manière qu'a le chercheur de considérer les problèmes à résoudre qui lui permet de s'adapter et de réussir. Un mathématicien possède tous les outils pour réussir en entreprise, habitué qu'il est à porter et développer une idée sur le long terme.

À condition toutefois de ne pas considérer une carrière dans le privé comme un choix par défaut. Un recruteur souhaite que le mathématicien qui postule ait envie de venir travailler avec eux. Un entrepreneur attend d'un candidat qu'il ait envie de venir dans son entreprise, qu'il ou elle sache ou se soit posé la question de savoir ce que cette entreprise fait, qu'il se soit posé la question de savoir ce qu'il ou elle pourrait apporter. Aller dans une entreprise, c'est vouloir résoudre le problème de cette entreprise. Ce que je cherche à savoir quand j'effectue un entretien d'embauche, c'est si le candidat a compris ce que cela veut dire que de travailler avec un autre rapport aux autres, un autre niveau de responsabilités, un autre rapport au temps, une autre image de soi-même. Il ne s'agit pas d'être publié dans une revue prestigieuse. Le plaisir se trouve dans le travail en équipe, dans le succès de l'entreprise.

Il faudrait qu'il existe plus de passerelles entre le monde académique et le secteur privé. Une expérience en entreprise, notamment dans une start-up, devrait être un élément naturel dans la carrière d'un mathématicien. Ce qui m'a donné le plus de plaisir depuis la création de *tinyclues*, c'est de me trouver dans une position d'aventure avec beaucoup d'incertitudes et un champ d'application gigantesque.

Prouver qu'une idée a de la valeur pour quelqu'un d'autre qui n'est pas spécialiste dans la vraie vie pourrait faire partir du rythme d'une carrière mathématique. Cette transition vers le monde de l'entreprise devrait être plus encouragée.

À ceux qui auraient encore des doutes, je n'ai qu'un conseil à donner : « Si cela vous intrigue, lancez-vous dans l'aventure. Il y a beaucoup de postes dans le privé pour les gens doués en mathématiques ! Les possibilités sont immenses ».

David Bessis a soutenu sa thèse à Paris 7 en 1998, sous la direction de Michel Broué. Après deux années à Yale, il a été recruté au CNRS en 2001. Ses travaux en algèbre et géométrie portent sur les groupes de réflexions complexes et les groupes de tresses associés, avec pour principal résultat la résolution d'une conjecture datant des années 1970 sur la topologie des arrangements de réflexions (*Finite complex reflection arrangements are K*$(\pi, 1)$, à paraître dans Annals of Maths). Il est aussi l'auteur de deux récits, *Sprats et Ars Grammatica*, parus aux éditions Allia. David Bessis a créé la start-up *tinyclues* en 2010, elle compte aujourd'hui 20 salariés.

Le point de vue d'un établissement financier majeur

Cédric Puel, Directeur Marketing Analytics & Performance chez BNP Paribas Personal Finance (BNPP-PF), répond à nos questions sur l'apparition et le rôle des big data chez BNPP-PF.

Pourriez-vous nous décrire ce que représentent les « Big Data » pour vous, et les raisons pour lesquelles BNP Paribas Personal Finance s'y intéresse ?

BNPP-PF a bâti une grande partie de son avantage concurrentiel sur sa capacité à exploiter des données, tant côté risque (octroyer et dimensionner correctement un crédit) que marketing. C'est donc naturellement que le groupe explore depuis quelques années ce que nous appelons les « Bigger Data », qui ont pour nous une définition précise qui ne cherche pas à être alignée sur l'une des multiples définitions des *Big Data* que l'on peut rencontrer. Ainsi, pour BNPP-PF, le domaine du Bigger Data recouvre l'ensemble des données que nous n'utilisions pas usuellement ; notre ambition est d'exploiter davantage de données qu'avant, d'où le comparatif *bigger*. En d'autres termes, en plus des données clients traditionnellement en possession des organismes de financement, nous nous intéressons à présent à des données internes jusque-là inexploitées (contacts provenant du client y compris texte et voix…) ainsi qu'à des données externes (bases partenaires, open data, données issues du web…) en fonction de ce qui est légal et acceptable par nos clients, ce qui peut varier d'un pays à l'autre. Ceci requiert d'agir dans le cadre défini par la CNIL (en France) et par les organismes équivalents dans les autres pays où nous sommes présents.

Nous utilisons ces Bigger Data pour améliorer la connaissance de nos clients, notamment à des fins de sélection ou de ciblage fondées sur la prédiction des comportements : appétence au crédit, sensibilité au prix, besoin spécifique d'assurance, capacité à épargner, etc. Nous cherchons en particulier à dépasser les segmentations classiques, peu prédictives, afin de tendre vers un traitement unique de chaque client.

C'est la direction Marketing Analytics & Performance de BNPP-PF qui est en charge de ces travaux. Localisée à Paris, sa mission est d'améliorer à court ou moyen terme la performance financière des offres dans les 30 pays dans lesquels nous sommes présents. Elle réalise des tests commerciaux et des analyses pour le compte des équipes marketing et commerciales locales, puis préconise des orientations qui deviendront le nouveau *business as usual*.

L'analyse des données n'est pas un domaine nouveau. Qu'y a-t-il de différent dans ces « Big Data » ?

Les Bigger Data sont l'extension naturelle de nos travaux d'hier : nous cherchons toujours à mieux connaître nos clients, mais maintenant nous le faisons avec davantage de données. Ces dernières années, nous avons pris connaissance des nombreux résultats qui ont illustré la multitude d'articles parus sur les Big Data. Mais cela a longtemps relevé de l'anecdotique, du type « la largeur des trottoirs d'une ville est prédictive des intentions de vote » – ce qui nous a laissés assez sceptiques.

Au fur et à mesure, certaines expérimentations, relayées notamment des consultants venus nous proposer leurs services, ont contribué à notre réflexion sur ce sujet. Nous avons identifié au-delà de nos données traditionnelles des informations qui nous semblaient avoir un sens pour nous. Ce sont celles sur lesquelles nous travaillons aujourd'hui, de manière parfois encore artisanale, avec des méthodes que nous créons au fil de l'eau. Et nous restons très vigilants : nous ne voulons pas donner, nous aussi, l'impression de prédire un besoin client avec une largeur de trottoir !

Quelles sont les compétences qui sont sollicitées : statistique, informatique, programmation, ou juste une expertise tableur ?

Les équipes analytiques de BNPP-PF sont historiquement robustes ; rien qu'en France, les fonctions risque, marketing, finance et opérations disposent de 150 analystes aux spécialités variées. Côté Marketing Analytics, nous avions déjà, avant l'arrivée et la « mode » des Big Data, des équipes pluridisciplinaires pour le groupe BNPP avec des compétences pointues en statistique, en informatique décisionnelle, en finance, également sur le risque et les tests opérationnels (ce que nous appelons le *Test & Learn*, et qui s'apparente aux tests scientifiques des laboratoires pharmaceutiques : donner aléatoirement un médicament ou un placebo à une population significative pour déterminer l'effet réel du médicament).

Nous avons souhaité aller plus loin avec l'apparition de nouveaux types de données. Tout d'abord, le croisement de données très différentes nécessite par ailleurs de nouvelles compétences de data management. Par exemple, analyser les contacts clients requiert des liens entre des chroniques de contact (date, canal, motif…) qui sont des données plutôt traditionnelles mais dont la richesse et la structure varient énormément d'un client à l'autre, et des contenus de relation client (des messages texte ou des enregistrements vocaux) qui sont des données non structurées difficiles à faire entrer dans une base de donnée classique. Nos data scientists doivent donc acquérir une importante palette de compétences : restructurer des données pouvant avoir un nombre variable de champs, réaliser des analyses sémantiques automatisées (*text mining*), utiliser des technologies d'analyse vocale…

Par ailleurs, le grand nombre de données et la nécessité d'être réactif impose de raccourcir les délais d'analyse. Un score ne doit plus se faire à partir de 10 variables dans un délai de 2 mois, mais à partir de 200 variables et en 2 jours… voire instantanément pour certains. Ces contraintes poussent au développement d'algorithmes, qui effectuent eux-mêmes une partie de la réflexion auparavant réalisée par l'humain. Nous développons aujourd'hui nos propres algorithmes de segmentation, avec succès, ce qui nous pousse à vouloir renforcer notre savoir-faire en programmation et en modélisation statistique. Nous le faisons, autant que possible, en traitant un problème avec plusieurs méthodes que nous mettons en concurrence, afin de déterminer la plus efficace, car à ce stade, nous n'avons que très peu de certitudes ! Par exemple, lorsque nous réalisons une segmentation *d'uplift* [1], nous traitons les données avec notre algorithme génétique « fait maison » et avec des méthodes statistiques connues (Victor Lo, arbres de décisions CART ou CHAID, différences de 2 scores, …).

Pour l'instant, travaillons encore sur des outils traditionnels (SAS, Excel+VBA), ce qui ne nous permet pas de gérer toutes les données de manière fluide. Nous devons donc aussi apprendre à travailler avec des technologies plus adaptées aux gros volumes de données. À titre d'exemple, une base partenaire de comportements d'achat utilisée récemment (nous ayant servi à réaliser un score commercial / d'appétence à une offre) était six fois plus volumineuse que toutes les autres données disponibles en interne sur ces clients.

1. Les scores d'uplift sont devenus clefs pour nous : ils permettent de déterminer si l'on doit « agir » sur un client pour obtenir un comportement désiré ou si le client adoptera naturellement ce comportement. Par exemple, si le client a une faible probabilité d'acheter mon produit au prix standard, mais une forte probabilité de l'acheter à un prix promotionnel, alors « j'agis » en lui proposant le prix promotionnel. En revanche, si sa probabilité d'acheter au prix promotionnel n'est pas suffisamment supérieure à celle qu'il achète au prix standard, alors « je n'agis pas » et je ne baisse pas mon prix.

Est-ce que les informations que vous arrivez à extraire permettent d'affiner effectivement vos analyses ? Autrement dit, est-ce que les données « parlent » ?

La question fondamentale est la suivante : ces nouvelles données accroissent-elles suffisamment la connaissance client pour que cela justifie de les analyser ? En d'autres termes (plus financiers) : le coût incrémental d'acquisition et de gestion des Bigger Data est-il couvert par les gains additionnels générés ? Les données traditionnelles d'un établissement financier sont déjà très fournies. En effet, en fonction du prêt sollicité, on demande au client de nous communiquer des informations personnelles parfois très complètes ; cela va du trio basique « Nom – Prénom – Date de naissance » jusqu'à des informations plus riches comme le budget (revenus, charges, etc.) ou la structure familiale : ces informations sont absolument nécessaires à une pratique responsable du crédit. Ici commencent véritablement les difficultés pour nous : comment faire (et est-il possible de faire) mieux qu'avec toutes ces informations qui sont déjà en notre possession ? Il nous faut trouver des données différentes, et tout aussi riches. Les contacts entrants de nos clients, par exemple, sont un bon complément aux données traditionnelles. Nous commençons à analyser, client par client, les chroniques d'appels ou d'emails et l'activité sur l'Espace Client. Pour l'instant, chaque message est entendu ou lu par un chargé de clientèle qui adresse une question ou un besoin ou une frustration. Demain, l'assemblage de tous ces signaux devrait nous permettre, via des analyses statistiques et sémantiques, d'anticiper des besoins ou des frustrations qui ne sont pas explicités par le client.

À ce stade, les Bigger Data « parlent » un peu : les améliorations à l'activité existent, mais elles restent souvent marginales au regard de ce que l'on développe par ailleurs, grâce aux données traditionnelles. Sur un score marketing, ces données Bigger Data peuvent représenter jusqu'à un tiers du pouvoir prédictif, mais il n'y a pas encore de *breakthrough* – c'est-à-dire un type de données qui décuplerait le pouvoir prédictif de nos outils. Nous avons bon espoir avec certaines pistes !

À ce propos, pourriez-vous nous expliquer ce qui est spécifique selon vous à BNPP-PF et au crédit par rapport à d'autres entreprises ?

Un établissement financier doit, en plus de la confidentialité imposée par la loi, établir une forte relation de confiance avec ses clients, qui lui confient ou lui empruntent de l'argent – ce qui est, la plupart du temps, un acte autrement plus important que de faire une réservation d'hôtel ou d'acheter un livre. Nous sommes donc soucieux de n'utiliser que des données qui sont pertinentes à notre prise de décision, et dont l'utilisation pourrait être admise par le client, ce qui est loin d'être le cas chez tous les acteurs du web, par exemple.

Quelles sont les perspectives et débouchés pour des étudiants : à votre avis, est-ce une formation porteuse à moyen et long terme ?

Il ne fait aucun doute que les métiers analytiques en général (statisticiens, analystes financiers, programmeurs, spécialistes de la web analyse…), et tout ce qui concerne la Big Data en particulier, sera porteur longtemps : la valeur ajoutée est forte pour une entreprise (quelques salaires en plus pour des gains en résultats pouvant aller de dizaines de millions à potentiellement plusieurs milliards), de plus en plus de secteurs en ont besoin (téléphonie, assurance, pharmaceutique, robotique…) et le savoir-faire n'est pas facilement accessible. Deux autres familles de compétences sont néanmoins (absolument) nécessaires à la réussite professionnelle, dans le privé comme dans le public : la capacité à communiquer (oral, écrit, posture, réseau…) et une excellente compréhension du business sous-jacent. Malheureusement, ces compétences sont encore trop négligées par les profils analytiques, hormis dans les pays anglo-saxons. D'ailleurs, cause ou conséquence, les entreprises anglo-saxonnes ont une culture analytique bien plus forte que celles des autres pays – et c'est très vrai dans la banque et les services financiers !

Pourriez-vous faire un rapide état des lieux à l'international : la France est-elle à votre avis à la pointe de ces nouvelles questions ? La formation en France (masters professionnels et de recherche, grand nombre d'écoles d'ingénieurs, etc.) permettra-t-elle de répondre aux besoins en personnels (et est-ce que les jeunes français pourront espérer des postes à l'étranger), ou faut-il créer des formations spécifiques supplémentaires ?

Nos activités couvrent 30 pays sur les quatre continents ; nous avons donc une vision globale significative, mais encore à affiner, des savoir-faire scientifiques et des compétences Big Data en France et à l'étranger.

Le premier constat est que les formations scientifiques françaises restent à nos yeux parmi les meilleures du monde, même si nous intégrons à

présent davantage de collaborateurs étrangers (notamment Europe centrale, Afrique du nord, Russie, Turquie, Brésil, Inde, Chine : cette évolution suit naturellement l'emprunte géographique de BNP Paribas), dont les compétences en fin d'études sont également d'un très bon niveau.

Ensuite, il nous semble que les prestataires spécialistes de la data en France sont au niveau de ce qu'il semble se faire de mieux ailleurs. Par exemple – mais ça n'en est qu'un parmi de nombreux autres – nous avons récemment mis en concurrence quatre spécialistes data reconnus afin de réaliser un outil prédictif de nos volumes commerciaux en fonction des investissements marketing et médias réalisés et, bien entendu, de nombreuses données externes type Big Data. Les quatre prestataires (un américain, un britannique et deux français) ont utilisé des méthodes différentes, mais d'un niveau de sophistication et de robustesse équivalents... et aboutissant à des résultats sensiblement équivalents en termes de précision.

Notre vision des formations en France reste encore incomplète : nombre d'entre elles sont en train d'évoluer vers le Big Data, et nous manquons de recul pour connaître leur pertinence et leur efficacité. Néanmoins, nous observons avec intérêt les nouvelles formations autour du Big Data, vers lesquelles nous orientons certains de nos collaborateurs. De cette manière, nous devrions bientôt en savoir plus !

Cédric Puel est Directeur Marketing Analytics & Performance pour le groupe BNP Paribas Personal Finance. Ses activités portent sur l'optimisation des offres du groupe (tarification, mix d'offres, marketing direct...), via une approche pluridisciplinaire combinant des savoir-faire en tests opérationnels, analyse statistique, finance et risque.

À propos de BNPP-PF : BNPP-PF est leader du financement aux particuliers en France et en Europe au travers de ses activités de crédit à la consommation et de crédit immobilier. Filiale à 100% du groupe BNP Paribas, BNPP-PF compte plus de 20 000 collaborateurs et opère dans une trentaine de pays.

Encore une histoire de symétrie : les immeubles

• B. RÉMY

« (...), le mot immeuble était prononcé avec respect. »
Stendhal, Vie de Henry Brulard.

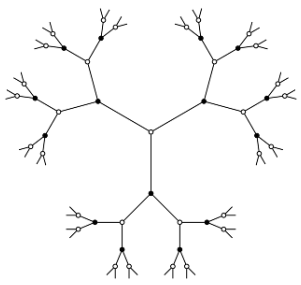
1. Première approche et premiers exemples

Ce texte présente une classe d'espaces à l'intersection de la théorie des groupes et de la géométrie : les *immeubles*. Il s'agit d'espaces singuliers puisque ce sont des recollements de simplexes ou de produits de simplexes. De ce fait ils ne relèvent pas de la géométrie différentielle au sens strict, mais ils possèdent (par définition) certaines propriétés de symétrie. On demande en effet qu'un immeuble soit réunion de sous-espaces tous isomorphes à un pavage donné au départ. Les copies de ce pavage sont appelées les *appartements* de l'immeuble en question, et on leur impose des propriétés d'intersection bien particulières (précisées et motivées au §3). En première approximation, on peut penser à un appartement comme à une coupe (ou à une tranche) dans un immeuble, sous-espace auquel on cherche le plus possible à se ramener pour y appliquer des idées géométriques élémentaires : convexité, usage de (produits de) réflexions etc. L'existence de symétries (au moins à l'intérieur des appartements) suggère que les immeubles admettent des actions de groupes très transitives. C'est souvent le cas et cela permet, en retour, de mieux comprendre les groupes qui agissent dessus.

Les arbres. Rappelons qu'un graphe est une réunion de segments (plutôt appelés des *arêtes*) recollés au niveau de leurs extrémités, les *sommets*. Un graphe est un *arbre* s'il est connexe et ne contient pas de boucle. La *valence* d'un sommet est le nombre d'arêtes qui contiennent ce sommet. Les arbres où chaque sommet est de valence $\geqslant 2$ (i.e. les arbres sans sommet cul-de-sac) sont des immeubles : ce sont en fait les immeubles infinis localement finis de dimension 1. Les sous-espaces qui jouent le rôle des appartements dans un arbre, vu comme un immeuble, sont les lignes droites : une telle droite est en effet « pavée » par les sommets des arêtes qu'elle contient. On peut toujours enrichir la structure d'un arbre en coloriant les sommets avec deux couleurs, de sorte qu'aux extrémités de toute arête chaque couleur apparaisse une fois exactement. On peut aussi munir l'arbre d'une métrique en décrétant chaque arête de longueur 1. On fera tout cela systématiquement dans ce texte. On peut enfin chercher à munir un arbre d'une action de groupe. Dans ce cas, il faut faire des hypothèses supplémentaires : en effet, en choisissant un arbre dans lequel les sommets ont des valences deux à deux distinctes, on obtient un immeuble de dimension 1... sans automorphisme. Par contre, dès lors qu'on suppose un arbre semi-homogène (tous les sommets de la même couleur ont la même valence), on peut démontrer que le groupe de ses isométries préservant les couleurs est un (très gros) groupe simple, c'est-à-dire sans sous-groupe distingué non trivial.

On peut penser aux immeubles comme à une généralisation des arbres en dimension supérieure.

FIGURE 1 – Une portion finie d'un arbre homogène de valence 3.



2. Modèles géométriques classiques

Une des motivations pour utiliser les immeubles est que ce sont des espaces susceptibles de recevoir des actions de groupes très transitives, ce qui permet de bien comprendre les groupes concernés. Cette motivation est d'autant plus forte que les groupes auxquels cette démarche s'applique appartiennent aux familles les plus utilisées, dans les branches les plus diverses des mathématiques. Typiquement, des groupes de matrices ; en termes plus précis, des groupes de Lie.

Les espaces symétriques. Pour mieux comprendre cela, on peut avoir en tête les modèles que les immeubles imitent : les espaces symétriques (riemanniens). De multiples définitions de ces espaces sont disponibles [3]. Pour ce qui nous intéresse principalement, il suffira de dire que ce sont des espaces homogènes G/K où G est un groupe de matrices (simple, non compact) à coefficients réels et K est un sous-groupe compact maximal de G. Le prototype d'espace symétrique est le quotient $\mathrm{SL}_n(\mathbf{R})/\mathrm{SO}(n)$, qui paramètre les produits scalaires normalisés sur $\mathbf{R}^n$; le cas particulier le plus populaire est celui où $n = 2$. En effet, on retrouve alors le demi-plan de Poincaré $\mathbf{H} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$: pour le voir, il suffit de faire agir les matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ de $\mathrm{SL}_2(\mathbf{R})$ sur $\mathbf{H}$ par homographie, i.e. en posant $\begin{pmatrix} a & b \\ c & d \end{pmatrix}.z = \dfrac{az+b}{cz+d}$. On vérifie que cette action est transitive sur $\mathbf{H}$ et que le stabilisateur du point i est le groupe $\mathrm{SO}(2)$.

Quels sont les points communs entre immeubles et espaces symétriques ?

Des propriétés de courbure. Les immeubles, espaces singuliers définis « par tranche » plutôt que localement, ne relèvent pas de la géométrie différentielle. Pourtant, ils admettent des distances qui en font des espaces métriques complets, et surtout avec de remarquables propriétés de courbure négative. Tout ceci est à comprendre dans un sens assez relâché [9] : d'une part, il existe une notion de segment géodésique et d'autre part, les triangles géodésiques sont plus fins que dans le plan euclidien (autrement dit, à longueurs de côtés deux à deux égales, les médianes sont plus courtes que dans la géométrie euclidienne). Toutes ces propriétés sont bien connues pour les espaces symétriques riemanniens et ont été abondamment exploitées dans ce cas.

Une situation très marquée de courbure négative pour les immeubles est justement fournie par les arbres. Dans ce cas, les triangles sont des tripodes (unions de trois segments partageant un sommet) ; en fait, les arbres sont à rapprocher des espaces hyperboliques, dans lesquels on peut vérifier que les triangles sont uniformément fins (voir le demi-plan de Poincaré $\mathbf{H}$). En quelque sorte, la non lissité des immeubles est compensée par le fait que ces espaces sont, métriquement parlant, des cousins des espaces symétriques riemanniens.

La théorie de Lie, le programme d'Erlangen et ses retournements. Un autre point commun entre immeubles et espaces symétriques est le fait que ces deux familles d'espaces sont très reliées à la théorie de Lie, le domaine des mathématiques qui étudie le phénomène de symétrie. Par exemple, les appartements d'un immeuble sont modelés sur un pavage donné d'une géométrie usuelle (euclidienne, sphérique, hyperbolique), ou sur une généralisation d'un tel pavage. Dans tous les cas, les appartements sont décrits par une version abstraite des groupes engendrés par des réflexions qu'on appelle les *groupes de Coxeter* [7, p. IV]. Dans les espaces symétriques, les sous-espaces plats maximaux (i.e. les plus gros sous-espaces sans courbure) admettent eux aussi une très utile partition en cônes euclidiens décrite par un groupe de réflexions fini, le *groupe de Weyl*.

La théorie de Lie intervient aussi et surtout au niveau des espaces tout entiers. La philosophie générale qui sous-tend ces considérations s'est développée à partir du fameux programme d'Erlangen de Felix Klein, qui (en gros) suggère d'étudier les géométries les plus régulières à travers leurs groupes de symétries [18] [1]. Par exemple, une des figures canoniques et imposées de l'agrégation a longtemps été de savoir classer les solides platoniciens grâce à la théorie des groupes. Des références pour aller plus loin dans ces considérations sont les livres récents et ludiques [13] et [14] de Ph. Caldero et J. Germoni.

1. Suivant un autre point de vue sur ces mêmes mathématiques, c'est aussi F. Klein qui fit recruter le cristallographe Schoenflies sur un poste de mathématiques appliquées à Göttingen.

La théorie de Lie fourmille de classifications. Elle classe tout ce qu'elle trouve, au moyen de données combinatoires élémentaires : des familles de groupes, de géométries et des produits dérivés (algèbres de Lie, représentations linéaires etc.). Il arrive que des classifications s'apparient naturellement en fonction de la philosophie ci-dessus : on passe d'une classification de groupes à une classification de géométries en prenant les espaces symétriques associés, et on fait le chemin inverse en prenant le groupe d'isométries des géométries considérées. Voici ce que le géomètre G.D. Mostow disait déjà de la théorie des immeubles au milieu des années 1970 [19, §16, p. 120] : « (...) Jacques Tits has succeeded in carrying out the Erlangen program in reverse. » Ce qu'il faut comprendre par là, c'est que les immeubles ont fourni le pendant géométrique de classifications de groupes qui préexistaient ; ils ont en quelque sorte comblé quelques cases vides dans le puzzle des classifications de la théorie de Lie.

3. Appartements et axiomes

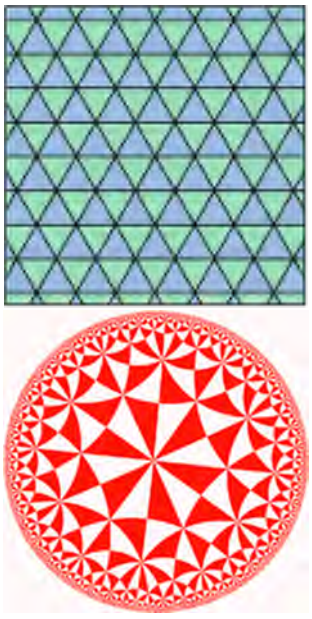
Venons-en maintenant à la définition des immeubles. En amont de la notion d'immeuble, il y a celle de *pavage*, c'est-à-dire (ici) de remplissage périodique d'un espace ambiant. Les principaux espaces pertinents pour ce qui va suivre sont les sphères, les espaces euclidiens et les espaces hyperboliques [2], mais ils n'épuisent pas toutes les possibilités. Le point de départ général est la notion de groupe de Coxeter. Un tel groupe, disons W, est donné par générateurs et relations (on parle de présentation de groupe) :

$$W = \langle s \in S \mid (st)^{M_{st}} = 1 \rangle$$

où S est un ensemble (supposé ici fini par commodité) et $M = [M_{st}]_{s\in S}$ est une matrice symétrique telle que $M_{ss} = 1$ et $M_{st} \in \mathbf{N}_{\geqslant 2} \cup \{\infty\}$ pour $s \neq t$. La présentation est très simple car elle ne fait que prescrire l'ordre des produits d'éléments. Ainsi $M_{ss} = 1$ dit que les générateurs canoniques sont des involutions, et l'on convient que $M_{st} = \infty$ ne prescrit rien du tout [3] sur l'ordre de st. Pour une matrice M comme ci-dessus, on peut toujours construire un complexe simplicial, appelé *complexe de Coxeter* et noté Σ_M ou Σ, sur lequel W agit comme un groupe de pavage [7, p. V.4]. Par exemple, les lieux de points fixes des générateurs canoniques s sont des espaces de codimension 1 bien compris.

Cependant, il est souvent plus efficace – et ce sera amplement suffisant pour fournir ici des exemples – de faire les choses dans l'autre sens, à savoir de partir d'un pavage convenable pour en tirer un groupe W. Donnons-nous dans une sphère, dans un espace euclidien ou dans un espace hyperbolique, un polytope dans lequel les angles entre faces de codimension 1 sont des sous-multiples entiers de π. On peut avoir en tête un triangle équilatéral dans le plan euclidien $\mathbf{R}^2$, un r-gone à angles droits ($r \geqslant 5$) ou triangle équilatéral d'angle $\frac{\pi}{4}$ dans le demi-plan supérieur $\mathbf{H}$... ou autre (le diviseur de π n'est d'ailleurs pas forcément toujours le même entier). Considérons le groupe W engendré par les réflexions par rapport à ces faces. Un théorème de Poincaré dit alors que W est un groupe de Coxeter et que le pavage obtenu en « translatant » le polytope de départ par W est une réalisation géométrique du complexe de Coxeter Σ.

Figure 2 – Des pavages mentionnés ci-dessous, qui peuvent servir d'appartements.



Avec ces dessins à l'esprit, nous avons tout ce qu'il faut pour définir les immeubles.

2. En termes riemanniens un peu plus savants, ce sont les espaces à courbure constante.
3. Au bout du compte, st est effectivement d'ordre infini (penser à une translation engendrée par deux réflexions parallèles).

Définition 1. Soient W un groupe de Coxeter et Σ son complexe de Coxeter. Un immeuble de type Σ est un complexe cellulaire [4] recouvert par des sous-complexes appelés appartements, tous isomorphes à Σ et satisfaisant aux axiomes suivants.

1. Deux facettes, c'est-à-dire deux cellules, sont toujours contenues dans un appartement.
2. Étant donnés deux appartements $\mathbb{A}$ et $\mathbb{A}'$, il existe un isomorphisme entre $\mathbb{A}$ et $\mathbb{A}'$ qui fixe l'intersection $\mathbb{A} \cap \mathbb{A}'$ point par point.

On appellera désormais W le *groupe de Weyl* de X.

Motivation métrique. Comment justifier de pareils axiomes ? Le mieux est peut-être de le faire de façon anachronique, c'est-à-dire en trichant sur les motivations historiques de J. Tits (qui était inspiré par les géométries d'incidence). Soit X un immeuble de type Σ. Supposons que le pavage Σ admette une distance invariante par le groupe de Weyl W (dans le théorème de Poincaré ci-dessus, c'est vrai par construction de Σ). On veut définir sur X une distance qui se restreigne à celle de Σ sur chaque appartement. Étant donnés deux points de X, l'axiome (i) dit que par un choix d'appartement les contenant, on peut obtenir une distance-candidate entre les points. Et modulo un peu de travail, l'axiome (ii) permet de montrer que la distance-candidate ne dépend pas du choix d'appartement. Il faut ensuite démontrer que l'application $X \times X \to \mathbf{R}_{\geqslant 0}$ ainsi obtenue est une distance (c'est le cas).

Des références pour aller plus loin dans les considérations générales sur les immeubles sont les livres d'Abramenko-Brown [1] et Ronan [23].

Lien avec la théorie géométrique des groupes. La théorie géométrique des groupes est le domaine des mathématiques qui consiste à étudier les groupes à travers des actions sur des espaces métriques avec de bonnes propriétés (par exemple, celles évoquées dans l'analogie ci-dessus entre immeubles et espaces symétriques). Cette discipline a connu un essor spectaculaire depuis que M. Gromov, dans les années 80, a montré que cette idée pouvait être poussée remarquablement loin, même dans des situations à première vue très dépouillées. Les immeubles fournissent des cas très particuliers puisque ce sont au contraire des espaces fortement structurés par la théorie de Lie. Cependant pour certaines questions ce sont de bons espaces-tests, une fois qu'on s'est assuré que des groupes intéressants agissent dessus (voir l'exemple des arbres sans automorphisme évoqué au début). En évoquant les questions de classification, on verra d'ailleurs que ce type de pathologie (absence d'automorphisme) n'est possible qu'en petite dimension pour les immeubles classiques (i.e. sphériques et euclidiens).

Les premiers groupes concernés. Dans une direction complémentaire, on peut se demander quels groupes peuvent agir de façon satisfaisante sur des immeubles. Par « satisfaisante » il faut comprendre que l'action permet de prouver des résultats de structure significatifs sur le groupe. Une notion qui s'est avérée pertinente est celle de *forte transitivité* : on suppose par cette condition que le groupe agit transitivement sur les inclusions d'une facette maximale, appelée *chambre*, dans un appartement. Autrement dit, à chaque fois que deux telles inclusions sont données, on peut trouver un élément du groupe qui envoie chambre sur chambre et appartement sur appartement [5]. Un des résultats importants de la théorie est que quand un groupe agit fortement transitivement sur un immeuble, il admet une structure combinatoire riche qu'on appelle *système de Tits* (ou BN-*paire*). C'est cette structure qui a permis à J. Tits de fournir une preuve uniforme de la simplicité des groupes de matrices classiques, modulo leur centre (et d'autres petites hypothèses) [7, p. IV.2.7]. Là encore, dans sa forme éclatée en cas particuliers, c'est un grand classique de l'agrégation... Retenons en tout cas qu'il y a une relation pour un groupe entre simplicité et action très transitive sur un immeuble, ce qu'on avait déjà évoqué pour les groupes d'automorphismes d'arbres.

De manière générale, les principaux exemples de groupes avec de bonnes actions sur des immeubles sont fournis par les groupes de matrices classiques (ou plus généralement, les groupes algébriques). Chacune des deux sections qui suivent va porter sur l'une des deux principales classes d'immeubles (sphériques et euclidiens). Ce sera l'occasion de résumer à grands traits des théories portant sur les groupes algébriques, dont les développements récents deviennent de plus en plus ardus techniquement et conceptuellement. La dernière section portera sur tous les autres immeubles, qu'on ap-

4. Écrire « cellulaire » permet de couvrir le cas des produits de complexes simpliciaux (dit polysimplicial).
5. On pourrait voir que cette notion est une survivance de la géométrie d'incidence dans la théorie.

pellera exotiques par commodité [6]. Les problèmes y sont moins structurés mais pas moins excitants, loin de là. On s'intéresse par exemple à des familles de groupes dont on attend des comportements nouveaux par rapport aux cas précédents, justement parce qu'on peut espérer (et parfois démontrer) que les groupes en question ne sont pas linéaires, c'est-à-dire ne sont sous-groupes d'aucun $\mathrm{GL}_n(K)$ quel que soit $n \geqslant 2$ et quel que soit le corps K.

4. Immeubles sphériques

Les *immeubles sphériques* sont les immeubles dans lesquels les appartements sont des pavages sphériques (i.e. pour lesquels le groupe de Weyl est fini). La classification de J. Tits [25] met en correspondance les immeubles sphériques de dimension $\geqslant 2$ avec les groupes de matrices simples [7]. C'est un exemple où, dans la théorie de Lie, une classification de géométries est appariée à une classification de groupes (voir §2). Plutôt que d'insister sur cet aspect classificatoire, nous allons passer en revue des applications des immeubles sphériques.

Théorème fondamental de la géométrie projective. La première application porte sur une généralisation du théorème fondamental de la géométrie projective. Étant donnée une application φ entre espaces projectifs qui respecte les sous-espaces linéaires et leurs intersections, ce théorème factorise φ en produit d'une application linéaire et d'un automorphisme des corps de base (pourvu que la dimension des espaces projectifs soit assez grande). Une des idées importantes de J. Tits est de voir l'immeuble sphérique d'un groupe de matrices simple comme une généralisation de l'espace projectif $\mathbb{P}^{n-1}(K)$ associé à $\mathrm{PGL}_n(K)$. Outre la classification des immeubles sphériques, cette famille d'idées a permis de dévisser les homomorphismes entre groupes de matrices (il faudrait dire entre groupes de points rationnels de certains groupes algébriques [6]).

Rigidité forte. Nous allons voir que ce dévissage a des conséquences importantes même dans le cas particulier où les coefficients des groupes de matrices sont des nombres réels. Pour cela, il nous faut parler d'un énoncé de géométrie différentielle, la rigidité de Mostow [19]. Le théorème de rigidité forte (de Mostow) s'intéresse aux variétés localement symétriques, c'est-à-dire celles dont le revêtement universel est un espace symétrique comme au §2. Il affirme qu'une variété localement symétrique de volume 1 et de dimension $\geqslant 3$ est complètement caractérisée par son groupe fondamental [8]. Autrement dit dans ce cas, la topologie détermine la structure métrique. Pour faire le lien avec les immeubles, on a besoin de parler de bord à l'infini.

Le bord des espaces symétriques. Sur l'ensemble des rayons géodésiques tracés dans un espace symétrique, on peut définir une relation d'équivalence qui identifie deux tels rayons quand ceux-ci restent à distance bornée l'un de l'autre [9]. L'ensemble des classes d'équivalence admet une topologie naturelle qui est compacte, et il peut être recollé à l'espace symétrique afin de compactifier ce dernier. Un fait remarquable est que le bord de l'espace symétrique G/K est un immeuble sphérique, précisément l'immeuble sphérique que la classification de Tits associe au groupe d'isométries G [3]. Revenons à la rigidité forte et partons d'un isomorphisme $\bar{\varphi}$ entre les groupes fondamentaux de deux variétés localement symétriques. Pour résumer très schématiquement la preuve (qui fait l'objet d'un livre entier [19]), on déduit de $\bar{\varphi}$ d'abord une application « grossièrement lipschitzienne » entre les espaces symétriques revêtant les deux variétés comparées (on parle de *quasi-isométrie*), puis une application φ entre les immeubles à l'infini des espaces symétriques. La troisième étape de la preuve consiste à appliquer à φ la généralisation du théorème fondamental de la géométrie projective pour en déduire une isométrie entre les espaces symétriques.

5. Immeubles euclidiens

Les *immeubles euclidiens* sont les immeubles dans lesquels les appartements sont des pavages euclidiens ; dans la littérature, on parle aussi d'immeubles *affines*. Le groupe de Weyl est alors extension d'un groupe de réflexions fini par un groupe abélien libre (formé de translations). Pour cette classe d'immeubles, les groupes pertinents sont

6. Parmi eux figurent des classes déjà assez bien comprises comme les immeubles hyperboliques, i.e. dans lesquels les appartements sont des pavages à courbure –1.
7. En termes plus techniques, avec la théorie de structure des points rationnels des groupes réductifs, dite théorie de Borel-Tits [5].
8. On peut toujours normaliser le volume, mais en toute rigueur il faudrait faire des hypothèses d'irréductibilité.

les groupes de matrices $G(k)$ qui sont simples sur des corps k munis d'une valeur absolue satisfaisant à l'inégalité ultramétrique :
$|\lambda+\lambda'| \leqslant \max\{|\lambda|;|\lambda'|\}$ pour tous x et y dans k.[9]
Il est tout fait à suffisant d'avoir en tête, comme exemple de groupe $G(k)$, un groupe classique (disons SL_n ou un groupe d'automorphismes de forme bilinéaire ou hermitienne/sesquilinéaire) à coefficients dans le corps $\mathbf{Q}_p$ des nombres p-adiques.

Historique. La section qui précède garantit qu'on dispose déjà d'une action fortement transitive (§3) du groupe considéré sur un immeuble sphérique. Dans les années 60, la mise en évidence (dans des groupes $G(k)$ particuliers) de systèmes de Tits à groupe de Weyl infini a conduit F. Bruhat et J. Tits à mettre en place une imposante machinerie dont le but principal était d'attacher à tout groupe algébrique sur un corps local un immeuble euclidien sur lequel le groupe agit fortement transitivement. Les motivations pour la théorie de Bruhat-Tits étaient nombreuses : preuve uniforme d'analogues de décompositions bien connues pour les groupes de Lie réels (Cartan, Iwasawa), classification de sous-groupes compacts maximaux... Il faut aussi avoir en tête qu'au même moment les spécialistes de théorie des représentations, ou d'analyse harmonique non commutative à la Harish Chandra, commençaient à s'intéresser aux groupes de Lie non archimédiens avec de sérieuses questions arithmétiques en arrière plan (voir comment l'article de présentation générale [27] s'insère dans des actes principalement consacrés aux formes automorphes).

Exemple. L'exemple le plus indiqué pour cette théorie est le groupe $\mathrm{SL}_n(\mathbf{Q}_p)$. Dans ce cas, on peut donner une définition concrète de l'immeuble euclidien associé, complètement analogue à celle de l'espace symétrique de $\mathrm{SL}_n(\mathbf{R})$ (§2). En effet, on a vu que cet espace symétrique est l'ensemble $\mathrm{SL}_n(\mathbf{R})/\mathrm{SO}(n)$ des produits scalaires normalisés sur $\mathbf{R}^n$. Si V est un $\mathbf{Q}_p$-espace vectoriel de dimension n, on dispose de la notion de norme ultramétrique sur V. On peut voir alors [10, §10] que l'ensemble des classes d'homothéties de normes non archimédiennes sur V est un immeuble euclidien de dimension $n-1$. Le groupe de Weyl est un groupe de réflexions affine de partie vectorielle le groupe symétrique sur n lettres et de sous-groupe de translations un groupe abélien libre de rang $n-1$. L'action de $\mathrm{SL}_n(\mathbf{Q}_p)$ sur les normes de V (par précomposition) permet de prouver les décompositions de Cartan et d'Iwasawa, à savoir dans ce cas :

$$\mathrm{SL}_n(\mathbf{Q}_p) = K\overline{T}^{+}K \quad \text{et} \quad \mathrm{SL}_n(\mathbf{Q}_p) = KTU,$$

où K est le sous-groupe compact (maximal) $\mathrm{SL}_n(\mathbf{Z}_p)$, le groupe U est formé des matrices trianguaires supérieures à coefficients diagonaux égaux à 1, le groupe T est formé des matrices diagonales à coefficients de la forme p^m et $\overline{T}^{+}$ est le sous-semi-groupe de T pour lequel les exposants $m \in \mathbf{Z}$ sont ordonnés de façon décroissante.

Les deux parties de la théorie de Bruhat-Tits. Cette théorie se découpe grosso modo en deux parties, chacune correspondant à un des deux gros articles publiés en 1972 et 1984 (voir aussi [24]). La première partie [10] ne fait pas du tout usage de théorie des groupes algébriques, c'est un mélange de pure théorie des groupes abstraits et de géométrie (combinatoire et métrique) des immeubles euclidiens. On y apprend comment déduire des décompositions d'Iwasawa et de Cartan d'une action fortement transitive sur un immeuble euclidien. La seconde partie de la théorie [11] traite des structures entières du groupe $G(k)$ en question, c'est-à-dire des façons de choisir des équations à coefficients dans l'anneau de valuation k° de k pour définir G comme groupe de matrices algébrique[10]. Il y a de multiples façons de trouver de telles équations de sorte que les solutions à coefficients dans k redonnent $G(k)$, mais une famille particulièrement intéressante, disons $\{\mathcal{G}_F\}$, est justement paramétrée par les facettes F de l'immeuble de Bruhat-Tits. Ces structures entières sont délicates à construire ; ce sont à la fois des outils cruciaux dans la stratégie de Bruhat-Tits et des objets qui ont eu de multiples usages depuis, notamment pour les groupes arithmétiques [21] et en théorie des représentations [20].

Analogie avec les espaces symétriques. On a déjà dit que même si ce sont des espaces singuliers, les immeubles de Bruhat-Tits ont les mêmes propriétés métriques que les espaces symétriques riemanniens non compacts (courbure

9. En termes techniques, un tel corps est appelé corps non archimédien, et on s'intéresse aux groupes de points rationnels $G(k)$ d'un groupe réductif G défini sur un corps valué non archimédien k.
10. L'anneau k° est un anneau local, décrit aussi comme la boule unité au sens large de la valeur absolue de k, la boule unité au sens strict étant l'idéal maximal de k°.

négative ou nulle, contractibilité géodésique). À ce titre, ils ont permis des calculs de cohomologie pour une vaste classe de groupes discrets, les groupes S-arithmétiques [4]. Pour toutes ces raisons et d'autres, on dit parfois que les immeubles de Bruhat-Tits sont les analogues non-archimédiens des espaces symétriques [11]. Enfin, les immeubles de Bruhat-Tits possèdent eux aussi un bord à l'infini (défini comme précédemment), qui est l'immeuble sphérique du groupe $G(k)$ quand on oublie que k a une valeur absolue. Ce bord permet encore de prouver un résultat de rigidité forte à la Mostow et c'est aussi le principal outil permettant de réduire la classification des immeubles affines à celle des immeubles sphériques [26] ; cette classification est présentée sous le point de vue des groupes classiques (i.e. sans groupe algébrique) dans le livre de R. Weiss [28].

6. Immeubles exotiques

Le terme d'*immeuble exotique* ne veut rien dire de précis pour les spécialistes, mais convenons ici qu'il s'agit des immeubles qui ne sont ni sphériques, ni euclidiens. C'est une définition qui vaut bien celle des verbes du troisième groupe en conjugaison, et elle a au moins la vertu de suggérer clairement ce qu'on attend de ces espaces : du neuf.

Analogie avec les situations précédentes. L'intérêt des groupes définis comme groupes d'isométries d'immeubles exotiques est qu'ils ne sont pas linéaires a priori (la linéarité peut être une obstruction à la simplicité – voir plus bas). C'est aussi ce qui fait la difficulté de leur étude : la boîte à outils disponible se réduit considérablement puisque les techniques de groupes algébriques ne peuvent plus être mises à profit comme auparavant, du moins directement. Cependant, il n'est pas interdit de voir un immeuble à groupe de Weyl infini, muni d'une métrique complète à courbure négative (qui existe toujours), comme une généralisation d'espace symétrique riemannien non compact. Au niveau des groupes, l'ensemble de toutes les isométries apparaît alors comme un analogue de groupe de Lie et les groupes qui opèrent avec stabilisateurs finis peuvent être comparés à des sous-groupes discrets de groupes de Lie. Ces analogies suggèrent de nombreux énoncés, et dans pas mal de situations intéressantes ces énoncés sont devenus en effet des théorèmes. Par exemple, des calculs très poussés de cohomologie de groupes d'automorphismes complets d'immeubles ont été obtenus en toute généralité [16], la simplicité abstraite de certains de ces groupes a été démontrée [17] et la rigidité des quasi-isométries (i.e., une rigidité impliquant la rigidité de Mostow) a été obtenue pour une classe d'immeubles dans lesquels les appartements sont des pavages hyperboliques [8].

Différences avec les situations précédentes. De façon complémentaire à ces analogies, de nouveaux phénomènes sont apparus dans l'étude des groupes qui opèrent sur des immeubles (encore une fois, pourvu qu'on s'assure que les groupes sont assez gros). Rappelons qu'un groupe Γ est dit *résiduellement fini* si l'intersection de ses sous-groupes d'indice fini est triviale : $\bigcap_{[\Gamma:\Delta]<\infty} \Delta = \{1\}$. Par une astuce classique, il est équivalent de demander que l'intersection des sous-groupes *distingués* d'indice fini soit triviale : un groupe infini résiduellement fini ne peut donc être simple. Or les groupes linéaires de type fini (autrement dit, les groupes engendrés par un ensemble fini de matrices) sont résiduellement finis... Tous ces faits mis bout à bout montrent qu'il est inutile d'espérer construire, au moyen de groupes de matrices, des groupes infinis, de type fini *et* simples. L'idée est donc de travailler sur des groupes qui opèrent par isométries avec stabilisateurs finis sur des immeubles exotiques. On peut prendre par exemple des groupes fondamentaux de complexes cellulaires finis, en s'assurant (par des conditions locales) que le revêtement universel est un immeuble.

L'intérêt de la situation est qu'elle est à bonne distance de la situation classique : elle conduit à étudier des objets (groupes et géométries) résolument nouveaux, en s'appuyant sur des intuitions– éventuellement des techniques – qui ont fait leurs preuves pour les groupes de Lie et leurs sous-groupes. On vient de voir que des arguments de groupes de matrices sont typiquement inopérants, mais des arguments de représentations unitaires, de théorie ergodique ou de courbure négative s'avèrent transposables.

Constructions de groupes simples. M. Burger et Sh. Mozes ont eu l'idée de regarder des complexes

11. Mais il faut alors avoir en tête que d'autres espaces (analytiques non archimédiens) peuvent prétendre à cette terminologie ; en fait, les uns et les autres ne sont pas sans rapport puisque souvent les espaces symétriques analytiques non archimédiens se rétractent naturellement sur des immeubles de Bruhat-Tits [2, Part V].

obtenus comme recollements finis de carrés (produits d'intervalles unité) : en s'y prenant bien, le revêtement universel est un produit de deux arbres homogènes, qu'on voit comme généralisation du produit de deux disques hyperboliques, ou encore de deux arbres de Bruhat-Tits. Une très belle combinaison d'analogie conceptuelle avec la situation classique (il s'agit quand même d'adapter ici une partie des travaux de Margulis sur les réseaux des groupes de Lie !), d'usages astucieux d'arithmétique et de groupes finis et profinis, leur permet alors de prouver le théorème suivant [12].

Théorème 1. *Il existe une infinité de groupes simples, de présentation finie, sans torsion. Ces groupes agissent librement sur des produits d'arbres avec une unique orbite de sommets.*

La beauté d'un tel résultat réside dans l'écart entre la grande accessibilité de l'énoncé et la difficulté de la preuve [12]. Le lecteur motivé pourra se convaincre de la force de l'énoncé d'existence en essayant de construire à la main des groupes simples infinis et de type fini [12]. La construction d'autres familles de groupes simples agissant discrètement sur des produits d'immeubles (de dimension supérieure cette fois) peut être obtenue au moyen de la théorie de Kac-Moody [15]. En ce qui concerne les immeubles exotiques, un texte de survol un peu plus détaillé sur cet aspect est [22].

Références

[1] P. Abramenko et K. S. Brown. *Buildings*. **248**. Graduate Texts in Mathematics. Theory and applications. Springer, New York, 2008, p. xxii+747. ISBN : 978-0-387-78834-0. DOI : 10.1007/978-0-387-78835-7. URL : http://dx.doi.org.docelec.univ-lyon1.fr/10.1007/978-0-387-78835-7.

[2] V. G. Berkovich. *Spectral theory and analytic geometry over non-Archimedean fields*. **33**. Mathematical Surveys and Monographs. American Mathematical Society, Providence, RI, 1990, p. x+169. ISBN : 0-8218-1534-2.

[3] L. Bessières, A. Parreau et B. Rémy, éds. *Géométries à courbure négative ou nulle, groupes discrets et rigidités*. **18**. Séminaires et Congrès. Société Mathématique de France, Paris, 2009, p. xxvi+466. ISBN : 978-2-85629-240-2.

[4] A. Borel et J.-P. Serre. « Cohomologie d'immeubles et de groupes *S*-arithmétiques ». *Topology* **15**, n° 3 (1976), p. 211–232. ISSN : 0040-9383.

[5] A. Borel et J. Tits. « Groupes réductifs ». *Inst. Hautes Études Sci. Publ. Math.* n° 27 (1965), p. 55–150. ISSN : 0073-8301.

[6] A. Borel et J. Tits. « Homomorphismes "abstraits" de groupes algébriques simples ». *Ann. of Math. (2)* **97** (1973), p. 499–571. ISSN : 0003-486X.

[7] N. Bourbaki. *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitres IV-VI*. Actualités Scientifiques et Industrielles, No. 1337. Hermann, Paris, 1968, 288 pp.

[8] M. Bourdon et H. Pajot. « Rigidity of quasi-isometries for some hyperbolic buildings ». *Comment. Math. Helv.* **75**, n° 4 (2000), p. 701–736. ISSN : 0010-2571. DOI : 10.1007/s000140050146. URL : http://dx.doi.org/10.1007/s000140050146.

[9] M. R. Bridson et A. Haefliger. *Metric spaces of non-positive curvature*. **319**. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 1999, p. xxii+643. ISBN : 3-540-64324-9. DOI : 10.1007/978-3-662-12494-9. URL : http://dx.doi.org.docelec.univ-lyon1.fr/10.1007/978-3-662-12494-9.

[10] F. Bruhat et J. Tits. « Groupes réductifs sur un corps local ». *Inst. Hautes Études Sci. Publ. Math.* n° 41 (1972), p. 5–251. ISSN : 0073-8301.

[11] F. Bruhat et J. Tits. « Groupes réductifs sur un corps local. II. » *Inst. Hautes Études Sci. Publ. Math.* n° 60 (1984), p. 197–376. ISSN : 0073-8301.

[12] M. Burger et S. Mozes. « Lattices in product of trees ». *Inst. Hautes Études Sci. Publ. Math.* n° 92 (2000), 151–194 (2001). ISSN : 0073-8301. URL : http://www.numdam.org/item?id=PMIHES_2000__92__151_0.

[13] P. Caldero et J. Germoni. *Histoires hédonistes de groupes et de géométries*. **1**. collection Mathématiques en devenir. Calvage et Mounet, 2013.

[14] P. Caldero et J. Germoni. *Histoires hédonistes de groupes et de géométries*. **2**. collection Mathématiques en devenir. Calvage et Mounet, 2015.

[15] P.-E. Caprace et B. Rémy. « Simplicity and superrigidity of twin building lattices ». *Invent. Math.* **176**, n° 1 (2009), p. 169–221. ISSN : 0020-9910. DOI : 10.1007/s00222-008-0162-6. URL : http://dx.doi.org/10.1007/s00222-008-0162-6.

[16] J. Dymara et T. Januszkiewicz. « Cohomology of buildings and their automorphism groups ». *Invent. Math.* **150**, n° 3 (2002), p. 579–627. ISSN : 0020-9910. DOI : 10.1007/s00222-002-0242-y. URL : http://dx.doi.org/10.1007/s00222-002-0242-y.

12. En gardant en tête, comme on l'a expliqué plus haut, qu'il est inutile de manipuler des groupes de matrices.

[17] F. Haglund et F. Paulin. « Simplicité de groupes d'automorphismes d'espaces à courbure négative ». In : *The Epstein birthday schrift*. Vol. 1. Geom. Topol. Monogr. Geom. Topol. Publ., Coventry, 1998, 181–248 (electronic). DOI : 10.2140/gtm.1998.1.181. URL : http://dx.doi.org/10.2140/gtm.1998.1.181.

[18] F. Klein. « Considérations comparatives sur les recherches géométriques modernes ». *Ann. Sci. École Norm. Sup. (3)* **8** (1891), p. 87–102. ISSN : 0012-9593. URL : http://www.numdam.org/item?id=ASENS_1891_3_8__87_0.

[19] G. D. Mostow. *Strong rigidity of locally symmetric spaces*. Annals of Mathematics Studies, No. 78. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1973, p. v+195.

[20] A. Moy et G. Prasad. « Unrefined minimal *K*-types for *p*-adic groups ». *Invent. Math.* **116**, n° 1-3 (1994), p. 393–408. ISSN : 0020-9910. DOI : 10.1007/BF01231566. URL : http://dx.doi.org.docelec.univ-lyon1.fr/10.1007/BF01231566.

[21] G. Prasad. « Volumes of *S*-arithmetic quotients of semi-simple groups ». *Inst. Hautes Études Sci. Publ. Math.* n° 69 (1989). With an appendix by Moshe Jarden and the author, p. 91–117. ISSN : 0073-8301. URL : http://www.numdam.org/item?id=PMIHES_1989__69__91_0.

[22] B. Rémy. « On some recent developments in the theory of buildings ». *actes ICM Séoul 2014* (à paraître).

[23] M. Ronan. *Lectures on buildings*. **7**. Perspectives in Mathematics. Academic Press, Inc., Boston, MA, 1989, p. xiv+201. ISBN : 0-12-594750-X.

[24] G. Rousseau. *Immeubles des groupes réductifs sur les corps locaux*. Thèse de doctorat, Publications Mathématiques d'Orsay, No. 221-77.68. U.E.R. Mathématique, Université Paris XI, Orsay, 1977, ii+205 pp. (not consecutively paged).

[25] J. Tits. *Buildings of spherical type and finite BN-pairs*. Lecture Notes in Mathematics, Vol. 386. Springer-Verlag, Berlin-New York, 1974, p. x+299.

[26] J. Tits. « Immeubles de type affine ». In : *Buildings and the geometry of diagrams (Como, 1984)*. Vol. 1181. Lecture Notes in Math. Springer, Berlin, 1986, p. 159–190. DOI : 10.1007/BFb0075514. URL : http://dx.doi.org.docelec.univ-lyon1.fr/10.1007/BFb0075514.

[27] J. Tits. « Reductive groups over local fields ». In : *Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 1*. Proc. Sympos. Pure Math., XXXIII. Amer. Math. Soc., Providence, R.I., 1979, p. 29–69.

[28] R. M. Weiss. *The structure of affine buildings*. **168**. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 2009, p. xii+368. ISBN : 978-0-691-13881-7.

Bertrand Rémy

École polytechnique, Centre de Mathématiques Laurent Schwartz.

bertrand.remy@polytechnique.edu

http://bremy.perso.math.cnrs.fr

Bertrand Rémy est professeur des universités. Sa spécialité est la théorie des groupes, précisément les actions sur diverses sortes d'espaces pour mieux comprendre ceux-ci.

Un grand merci à Boris Adamczewski, Sébastien Gouëzel, Romain Tessera et au rapporteur pour leurs remarques et encouragements très amicaux.

Discrétion assurée ?

- A. Joux
- C. Pierrot

« Je ne peux pas vous le dire à tous à la fois, et si vite que ça. Parce qu'un secret, ce n'est pas quelque chose qui ne se raconte pas. Mais c'est une chose qu'on se raconte à voix basse, et séparément. »

César [1]

Depuis un autre César et son célèbre chiffrement, les « codes secrets » intriguent, la cryptographie fascine. Entrez dans la confidence et cheminons ensemble à la découverte de cette science du secret. Comment ? Grâce aux différentes facettes d'un problème à l'intersection de la théorie des nombres et de l'algorithmique : le problème du logarithme discret.

Soient $(G,\times)$ un groupe cyclique et g un générateur de G. Considérons alors $x \mapsto g^x$, l'exponentiation discrète à la puissance x en base g, x étant un entier. Cette opération partage de nombreuses propriétés avec l'exponentiation ordinaire, comme l'égalité $g^{x+y} = g^x \cdot g^y$. L'inverse de cette opération consiste, étant donné un élément h dans G, à déterminer un entier x tel que :

$$h = g^x.$$

L'exponentiation discrète étant périodique, de période $|G|$, cet entier x n'est pas unique. En revanche $x \bmod |G|$ est bien déterminé : il sera appelé le *logarithme discret* de h en base g et noté $\ln_g(h)$. Par abus de langage, on confondra souvent ce logarithme avec son unique représentant dans l'intervalle $[0,|G|-1]$. Comme pour les logarithmes classiques :

$$\ln_g(h\cdot j) \equiv \ln_g(h) + \ln_g(j) \pmod{|G|}.$$

On considère que le problème du logarithme discret est résolu dans un groupe G dès lors que pour tout élément de G il est possible de déterminer efficacement son logarithme discret (ou l'un de ses représentants). Lorsque l'ordre de G est connu, résoudre le problème du logarithme discret dans G, c'est simplement expliciter l'isomorphisme :

$$\begin{array}{ccc} \mathbb{Z}/|G|\mathbb{Z} & \to & G \\ x & \mapsto & g^x \end{array}$$

sous une forme calculatoirement efficace. Les récentes découvertes à ce sujet que l'on se propose de vous raconter ont eu un impact conséquent en cryptographie.

Mais... quel est le rapport vous demandez-vous ?

1. Logarithmes discrets et cryptographie

Au début du siècle dernier, Kraïtchik [12, Chap. V] manipulait déjà notre logarithme discret x, qu'il appelait l'indice de g^x dans le groupe ; ce qui valu, au passage, le nom de la méthode sur laquelle nous nous appuyons, la méthode du calcul d'indice. Toutefois, la réelle notoriété de ce problème remonte à la naissance de la cryptographie moderne.

À la recherche des problèmes difficiles. Lorsque vous souhaitez chiffrer et déchiffrer des messages (plus ou moins) secrets, signer un document numérique ou vous authentifier auprès de votre banque, vous [2] utilisez des techniques (ou *cryptosystèmes*) construites à partir d'hypothèses calculatoires réputées difficiles. Bien choisir ces hypothèses est plus délicat qu'il n'y paraît : il faut disposer d'un problème difficile à résoudre pour un attaquant alors que le déchiffrement doit être facile pour un utilisateur légitime muni de la bonne clef. Il nous faut donc disposer d'un cryptosystème pour lequel il est difficile de trouver la bonne clef, alors que par construction il est nécessairement facile de tester si une clef donnée est correcte. Du point de vue de la théorie de la complexité, cela veut dire que la cryptographie ne peut exister que

1. Marcel Pagnol, *César*, Livre de Poche n° 161, p. 115.
2. Pris au sens large, la tâche est généralement déléguée à votre ordinateur ou à votre carte bancaire.

si deux classes [3] bien connues **NP** (notre problème est dans **NP** car il est facile de tester si une clef est correcte) et **P** (on ne le veut pas dans **P** pour que la bonne clef ne se trouve pas facilement) sont distinctes. Or, cette question n'est pas résolue. Pire, elle est considérée comme le problème ouvert le plus important du domaine, à un point tel qu'elle fait partie des sept problèmes à 1 million de dollars du *Clay Millenium Challenge*.

Par conséquent, on ne sait pas aujourd'hui s'il existe de véritables problèmes difficiles sur lesquels appuyer les fondements de la cryptographie. On ne peut que choisir des problèmes qui ont été suffisamment étudiés pour que l'absence de solution soit un bon indice de leur difficulté. Pour cette raison, la cryptographie à clef publique repose généralement sur des problèmes issus des mathématiques. Par ailleurs, l'essentiel des calculs se fait sur des ordinateurs qui préfèrent manipuler un monde d'objets discrets plutôt qu'un monde continu. C'est ainsi que le vaste champ de la théorie des nombres nous fournit deux candidats incontournables : le problème de la factorisation des entiers et celui du logarithme discret.

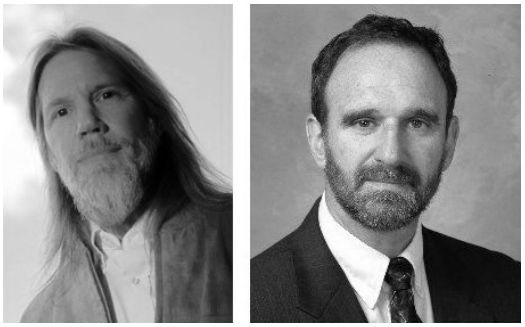
Les projecteurs se tournèrent en 1976 sur nos logarithmes, discrets jusque là, lorsque Diffie et Hellman proposèrent un mécanisme d'échange de clef entre deux personnes [5], sans connaissance d'un secret commun préalable. La cryptographie à clef publique était née ! Pour bien comprendre l'impact de ce résultat, très simple à expliquer par ailleurs, il faut se rappeler que, des siècles durant, de Jules César à la Seconde Guerre Mondiale, tous les échanges d'informations sensibles nécessitaient… un échange préalable, celui de la clef *secrète* du protocole. Le serpent se mordait la queue : comment communiquer de manière sécurisée avec quelqu'un que l'on n'avait jamais vu auparavant ? L'introduction de la cryptographie à clef publique grâce au logarithme discret permit de contourner cet écueil millénaire.

Échange de clefs de Diffie-Hellman. Si nous souhaitons créer une clef secrète commune en suivant le protocole de Diffie et Hellman, nous nous accordons tout d'abord sur un groupe cyclique G et un générateur g. Antoine choisit ensuite secrètement un entier a uniformément dans l'intervalle $[0, |G|-1]$, puis calcule g^a, qu'il envoie à Cécile sur un canal non sécurisé. De son côté, Cécile choisit de la même manière un entier aléatoire c et communique l'élément g^c à Antoine. Ainsi, chacun de nous deux est capable de calculer une valeur commune, à savoir :

$$(g^c)^a = g^{a\cdot c} = (g^a)^c$$

qui nous servira maintenant de secret commun.

Figure 1 – Whitfield Diffie et Martin Hellman.



La sécurité de ce système dépend de plusieurs hypothèses. Tout d'abord, il faut supposer qu'une tierce personne cherchant à mettre en défaut ce protocole se contentera d'écouter les communications sans chercher à les modifier. En effet, pour un attaquant actif, il est très aisé de parler à Cécile en se faisant passer pour Antoine et à Antoine en se faisant passer pour Cécile. De cette façon, il établit une clef commune avec chacun des deux de manière à faire suivre à son gré en les déchiffrant et rechiffrant tous les messages qui circuleront. En l'absence de secret commun préalable, nous ne nous rendrons compte de rien. C'est une faille bien connue de cet échange de clef (lorsqu'il est mal utilisé) que l'on appelle généralement *l'attaque par l'homme du milieu*.

Face à un attaquant passif, par exemple un lecteur indiscret, qui écouterait le canal et apprendrait donc g, g^a et g^c, que peut-on dire de la sécurité du système ? L'attaquant sera-t-il capable de calculer g^{ac} ? Pour que cela soit difficile, il est indispensable que le problème du logarithme discret le soit aussi. Sinon, il suffirait de calculer a (ou c), à partir de g^a, et d'en déduire le secret $g^{ac} = (g^c)^a$.

Peu après l'invention de l'échange de clef de Diffie et Hellman, Rivest, Shamir et Adleman [18] proposèrent une manière alternative de construire la cryptographie à clef publique en utilisant le problème de la factorisation des grands entiers. C'est

3. La classe **P** correspond aux problèmes résolubles en temps polynomial tandis que la classe **NP** regroupe ceux pour lesquels une solution, une fois donnée, est vérifiable en temps polynomial.

le fameux cryptosystème RSA, pouvant être utilisé soit pour chiffrer, soit pour signer des messages. Quelques années plus tard, ElGamal [6] montra qu'il était aussi possible de se baser sur le logarithme discret pour les mêmes utilisations.

Depuis, le logarithme discret reste un acteur majeur du domaine. Sa plus grande flexibilité figure parmi ses avantages. Il offre en effet plus de choix que la factorisation, puisqu'il autorise de nombreuses possibilités pour le groupe G : par exemple, le groupe des points rationnels d'une courbe elliptique (définie sur un corps fini) qui améliore en outre la sécurité du Diffie-Hellman. Sur une courbe elliptique générale, le problème est en effet plus difficile que dans un corps fini, dont la structure plus riche facilite la résolution. L'utilisation de telles courbes permet donc à niveau de sécurité égal de réduire la taille des clefs.

En près de quatre décennies, afin d'appréhender plus précisément la sécurité des protocoles cryptographiques, de nombreuses recherches se sont consacrées au calcul de logarithmes discrets. Deux grandes familles se distinguent :

- les algorithmes génériques, qui utilisent uniquement les opérations de groupe et la connaissance de $|G|$ et de sa factorisation,
- les algorithmes spécifiques, qui tirent parti de la description particulière du groupe considéré. La méthode du calcul d'indice donne ainsi un levier efficace principalement pour le cas des corps finis. Les récents progrès algorithmiques concernant les corps finis de petite caractéristique que nous aborderons plus loin font partie de cette famille.

2. Algorithmes génériques

À titre de comparaison future, il est bon d'introduire les algorithmes génériques qui n'utilisent pas la description spécifique du groupe G. Sans rentrer dans les détails, voici un bref point sur la question.

- La *méthode brutale* consiste simplement, pour retrouver le logarithme de h en base g, à énumérer les puissances successives $g^2, g^3, g^4, \cdots$ de g et à les comparer avec h. Sa complexité est en $O(|G|)$. Elle est bien entendu sans intérêt pratique.
- Les *méthodes en racine carrée*. Supposant connue la factorisation de $|G|$, Pohlig et Hellman (le même !) montrent en 1978 qu'il n'est pas plus compliqué de calculer des logarithmes dans G que dans tous ses sous-groupes d'ordre premier. Pour retrouver un logarithme discret dans le groupe tout entier, l'idée consiste à projeter l'élément dont on cherche le logarithme sur ses sous-groupes d'ordre premier, et à y calculer un petit nombre de logarithmes discrets dont l'assemblage fournira le résultat recherché. La même année, Pollard détaille comment résoudre le problème du logarithme discret dans un groupe d'ordre premier en $O(\sqrt{|G|})$ opérations : c'est la méthode Rho de Pollard. En combinant les algorithmes de Pohlig–Hellman [15] et Rho de Pollard [16], il est possible de calculer des logarithmes discrets en $O(\sqrt{p})$, où p est le plus grand facteur premier intervenant dans la factorisation de $|G|$.
- *Optimalité.* Shoup introduit en 1997 un cadre théorique, le modèle du groupe générique [19], pour étudier la complexité de ces algorithmes. Dans ce modèle, il montre qu'il n'est pas possible de descendre en dessous de la complexité en racine carrée obtenue par Pohlig, Hellman et Pollard. Notons que ces résultats d'optimalité ne s'appliquent pas pour les méthodes de calcul qui exploitent de façon fine la description de G.

3. Méthode du calcul d'indice

3.1 – Description générale

Cette méthode fonctionne aussi pour factoriser des entiers, mais nous ne nous intéresserons ici qu'au cas du logarithme discret, encore une fois dans un groupe cyclique G engendré par g. Les algorithmes de cette famille se découpent en plusieurs phases.

1. **Phase préliminaire.** Tout algorithme par calcul d'indice commence par fixer la description de G qui sera utilisée pour la suite, et qui peut différer de celle initialement fournie. Par exemple, on pourra choisir de travailler sur $\mathbb{F}_{2^4}$ vu comme $\mathbb{F}_2[Y,Z]/(Y^2+Y+1, Z^2+Z+Y)$ même s'il est initialement donné par $\mathbb{F}_2[X]/(X^4+X+1)$. On détermine aussi un sous-ensemble relativement petit d'éléments particuliers de G, que l'on nomme la base de lissité. Celle-ci est constituée d'éléments eux-même considérés comme petits, en un sens restant à définir.
2. **Phase de création de relations (ou phase de crible).** L'objectif de cette étape est de

créer un grand nombre de relations multiplicatives entre éléments de la base de lissité. Si la base utilisée est $\{g_i, i \in I\}$ nous nous intéresserons à des équations de la forme :

$$\prod_{i\in I} {g_i}^{m_i} = \prod_{i\in I} {g_i}^{n_i}. \qquad (1)$$

En prenant le logarithme discret de chacun des deux côtés nous en déduisons que :

$$\sum_{i\in I} m_i \ln_g g_i \equiv \sum_{i\in I} n_i \ln_g g_i \mod |G|.$$

On obtient ainsi une équation linéaire entre les logarithmes des g_i, qui sont nos inconnues. La phase de crible s'arrête lorsque l'on a récolté un nombre suffisant d'équations de cette forme, de sorte de pouvoir en extraire une solution unique (à constante multiplicative près). Autrement dit, le rang du système doit être égal au nombre d'inconnues moins un, modulo chacun des facteurs de $|G|$.

Notons qu'à l'issue de l'algèbre linéaire, puisque l'on obtient un élément arbitraire du noyau de la matrice, les logarithmes retrouvés ne le sont qu'à constante multiplicative près. Autrement dit, au lieu d'obtenir $\{\ln_g(g_i), i \in I\}$, on a $\{\lambda \ln_g(g_i), i \in I\}$ pour un certain λ. Toutefois, il est facile de retrouver les bons logarithmes, en supposant que g appartienne à la base de lissité – le logarithme de g, qui vaut 1, nous donnant la valeur de ce λ artéfact.

3. **Phase d'algèbre linéaire.** Cette étape cherche à résoudre le système linéaire issu des relations, afin d'obtenir les logarithmes discrets de tous les éléments de la base de lissité [4]. Une observation importante qui apparaît dans la plupart des algorithmes par calcul d'indice est la suivante : peu d'éléments interviennent dans chacune des relations, le système produit est donc *creux*. Cela accélère grandement l'algèbre linéaire car la complexité de l'algorithme de résolution est alors quadratique et non cubique comme dans le cas général.
4. **Calcul d'un logarithme individuel (ou phase de descente).** Afin de résoudre réellement le problème du logarithme discret dans G, nous devons pouvoir retrouver le logarithme d'un élément arbitraire et pas seulement des éléments de la base de lissité. Soit $z \in G$ un tel élément arbitraire et x son logarithme en base g. En quelques mots, l'idée consiste alors à décomposer z en produits d'autres éléments qui peuvent être considérés comme plus petits que lui. En itérant ce procédé, z s'exprime finalement comme produit d'éléments de la base de lissité $g^x = z = \prod_{i\in I} {g_i}^{\alpha_i}$. Puisque l'on connait les logarithmes discrets de ces derniers, on retrouve alors facilement x en écrivant $x = \sum_{i\in I} \alpha_i \ln g_i$.

3.2 – Lissité et complexité

Les algorithmes par calcul d'indice reposent sur l'idée de décomposer des éléments [5] comme produits d'éléments considérés comme petits. Les éléments qui peuvent se factoriser de cette manière sont dits *lisses*. Un problème essentiel pour l'analyse de ces algorithmes consiste donc à estimer la probabilité d'obtenir de tels éléments lisses. Dans de nombreux cas, on procède heuristiquement en supposant que les éléments créés se comportent comme des éléments aléatoires de même taille. Bien qu'inélégante, car non prouvée, cette heuristique a permis d'obtenir de nombreux progrès algorithmiques et a conduit à un grand nombre de factorisations explicites d'entiers et de calculs de logarithmes discrets.

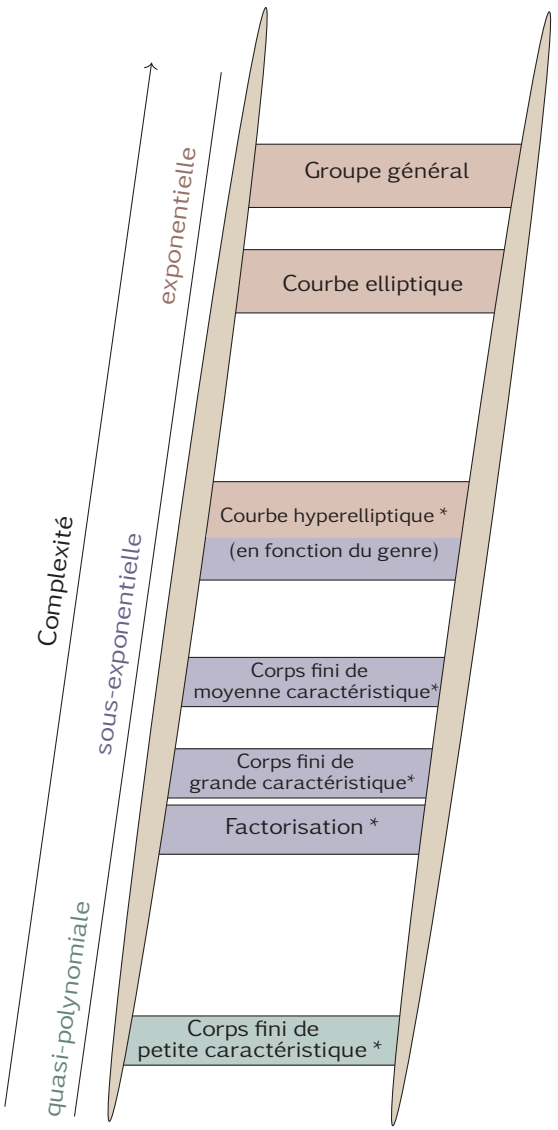
Dépendre d'une telle heuristique est inconfortable, et nous aimerions nous en abstraire. Pourtant, les algorithmes rigoureux qui existent actuellement se montrent bien moins efficaces que leurs homologues heuristiques. De manière tout à fait surprenante, les dernières avancées spectaculaires concernant les corps finis de petite caractéristique reposent justement sur le fait que, lorsque certaines heuristiques deviennent fausses (et que les éléments engendrés par la phase de création de relations ne se conduisent pas comme des éléments aléatoires), il devient possible de retourner cette faille à notre avantage.

La complexité des algorithmes par calcul d'indice s'exprime généralement avec une notation particulière qui provient justement des estimations de probabilité de lissité d'éléments aléatoires. Soyons un peu plus précis : un entier est dit y-lisse si tous ses facteurs premiers sont inférieurs à y tandis qu'un polynôme sur un corps fini est dit m-lisse si tous ses facteurs irréductibles sont de degré

4. Ou, au moins, une grande partie d'entre eux. En effet, certaines propriétés de la phase de crible peuvent mener à écarter quelques éléments de la base de lissité, qui ne seront présents dans aucune équation.
5. En pratique : des entiers, des idéaux ou des polynômes.

au plus m. Canfield, Erdös et Pomerance [4] calculèrent en 1983 les probabilités de lissité d'entiers. Une dizaine d'années plus tard, Panario, Gourdon et Flajolet [13] généralisèrent cette idée à la lissité d'un polynôme sur un corps fini.

FIGURE 2 – Echelle schématique des complexités asymptotiques actuelles de la factorisation et du problème du logarithme discret dans différents groupes. L'astérisque indique l'appartenance à la famille des algorithmes par Calcul d'Indice.



Ces deux résultats étonnamment proches l'un de l'autre peuvent se résumer ainsi : dans une large plage de paramètres, la probabilité qu'un entier aléatoire inférieur à x soit y-lisse (respectivement qu'un polynôme aléatoire de degré inférieur à n soit m-lisse) est $u^{-u+o(1)}$ où u est donné par $u = \ln x/\ln y$ (respectivement $u = n/m$). L'utilisation de ce résultat est simplifiée par la notation :

$$L_q(\alpha, c) = \exp\Big((c + o(1))(\ln q)^{\alpha}(\ln\ln q)^{1-\alpha}\Big)$$

où α et c sont des constantes telles que $0 \leqslant \alpha \leqslant 1$ et $c > 0$ et où $o(1)$ tend vers zéro pour $q \to \infty$. L'abréviation $L_q(\alpha)$ sera utilisée lorsque l'on voudra négliger c.

Dans la première phase d'un algorithme par calcul d'indice, le nombre d'opérations à effectuer est grossièrement égal au nombre de relations que l'on souhaite obtenir multiplié par l'inverse de la probabilité ; il est donc normal que l'on retrouve la notation L_q dans la complexité asymptotique finale de l'algorithme. Habituellement, q désigne le cardinal du groupe dans lequel nous souhaitons résoudre le problème du logarithme discret. Pour comparer un algorithme qui nécessite $L_q(\alpha, c)$ opérations au total à d'autres du même type, il faut d'abord étudier le premier paramètre, puisqu'il gouverne le passage d'un algorithme exponentiel (en temps) à un algorithme polynomial. Plus précisément, si α tend vers 1, $L_q(\alpha)$ devient exponentiel en la taille de q, c'est-à-dire en $\ln q$. Remarquez que $\ln q$ est le nombre de bits nécessaires pour encoder les éléments du groupe en question. Il est donc naturel que ce soit cette valeur que l'on considère lorsque l'on exprime la complexité des algorithmes. De même, lorsque α vaut 0, $L_q(\alpha)$ est *polynomial* en $\ln q$. On qualifie de *sous-exponentiel* tout algorithme de calcul de logarithme discret sur un groupe de taille q qui a une complexité en $L_q(\alpha)$ avec $0 < \alpha < 1$. De même, on qualifie de *quasi-polynomial* tout algorithme dont la complexité est en $L_q(o(1))$.

La Figure 2 donne une indication des complexités actuelles que l'on peut obtenir.

4. Calcul d'indice dans les corps finis

4.1 – La récolte des relations, une étape clef

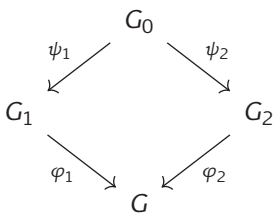
Les algorithmes de calcul d'indice reposant sur la construction de relations multiplicatives, les différentes méthodes pour obtenir de telles relations forment un fil conducteur dans l'historique du logarithme discret dans les corps finis.

Les premiers algorithmes en $L(1/2)$. Les premiers algorithmes de calcul d'indice pour les corps finis ont été proposés à la fin des années 70 par Adleman [1] pour les corps de cardinalité première. Par exemple, pour calculer le logarithme discret de u modulo un nombre premier p, l'approche la plus simple consiste à prendre un entier aléatoire a à calculer un représentant de u^a modulo p dans l'intervalle $[0, p-1]$ et à vérifier si

$$u^a \bmod p = \prod g_i$$

avec g_i des nombres premiers inférieurs à une certaine borne B. On obtient ainsi des relations dans une base de lissité formée des nombres premiers plus petits que B et de u. En supposant que g est bien dans la base de lissité, on obtiendra directement le logarithme recherché sans qu'une phase de descente ne soit nécessaire [6]. Notons que pour la plupart des valeurs de a, u^a ne sera pas B-lisse, et sera donc écarté. La complexité dépendra donc de la probabilité qu'un entier aléatoire inférieur à p soit B-lisse. Bien que primitive, cette approche permet déjà d'obtenir une complexité sous-exponentielle, de la forme $L_p(1/2)$. Elle se généralise à de nombreux corps finis et présente l'intérêt de fournir un algorithme probabiliste rigoureusement prouvé [17], contrairement aux autres algorithmes de la même famille, qui, bien que plus performants, reposent encore sur certaines hypothèses heuristiques.

La méthode du diagramme commutatif. Une idée essentielle pour améliorer la recherche de relations multiplicatives consiste à préalablement décrire le groupe G de façon à pouvoir l'inclure dans un diagramme commutatif de la forme suivante :



Dans ce diagramme commutatif, G_0, G_1 et G_2 sont des groupes bien choisis (la plupart du temps, il s'agit même d'anneaux) et toutes les applications sont des morphismes. Ainsi, pour tout x dans G_0, on obtient une égalité dans G :

$$\varphi_1(\psi_1(x)) = \varphi_2(\psi_2(x)).$$

Comme dans la description générale, il n'est gardé qu'une petite partie de ces relations. À cette fin, il faut distinguer dans chaque groupe intermédiaire G_1 et G_2 un petit sous-ensemble d'éléments, disons $B_1 \subset G_1$ et $B_2 \subset G_2$. Le sous-ensemble $\varphi_1(B_1) \cup \varphi_2(B_2)$ de G est alors la base de lissité de cet algorithme. Cela signifie que l'on ne conserve que les relations pour lesquelles $\psi_1(x)$ se décompose comme $\prod_{b_{1,i} \in B_1} b_{1,i}$ et $\psi_2(x)$ comme $\prod_{b_{2,i} \in B_2} b_{2,i}$. On obtient ainsi une relation entre produits dans G :

$$\prod_{b_{1,i} \in B_1} \varphi_1(b_{1,i}) = \prod_{b_{2,i} \in B_2} \varphi_2(b_{2,i}).$$

Cette méthode se révèle assez générale, mais les choix de G_0, G_1 et G_2 sont spécifiques à chaque type de groupe. Nous donnons un exemple concret de ces choix au paragraphe suivant. En 1984, Coppersmith obtient ainsi les premiers algorithmes de complexité $L_q(1/3)$ où q est la taille du corps considéré. Ce résultat, limité au cas des corps de caractéristique 2, est ensuite étendu progressivement à tous les corps finis. Ainsi, le crible par corps de fonctions permet de calculer des logarithmes dans tous les corps finis de petite caractéristique, tandis que le crible par corps de nombre (et ses variantes) concerne les corps de caractéristique moyenne à grande.

Petite, moyenne et grande caractéristiques. Il est probablement temps d'examiner cette notion de taille de caractéristique : en réalité, lorsque l'on parle de petite ou de grande caractéristique, on considère implicitement la taille *relative* de cette caractéristique avec celle du degré de l'extension, pour une taille de corps fixée. Ainsi, si l'on s'intéresse au corps fini $\mathbb{F}_{p^n}$ et que l'on souhaite évaluer la taille de sa caractéristique p, on commencera par écrire p sous la forme $p = L_{p^n}(l, c)$ avec $0 < l < 1$ et c une constante proche de 1. Si $l < 1/3$, on parlera de petite caractéristique, si $1/3 < l < 2/3$, de moyenne caractéristique, et de grande si $2/3 < l$.

4.2 – Corps de nombres ou corps de fonctions ?

Dans le diagramme commutatif, les groupes G_0, G_1 et G_2 donnent une représentation implicite du corps fini $G = \mathbb{F}_{p^n}$. G_1 et G_2 ne peuvent donc pas être tous les deux très petits. Cette restriction limite

6. Si g n'est pas dans la base, il est facile de l'ajouter en considérant des relations un peu plus générales $u^a g^b = \prod g_i$.

le choix de la base de lissité et la forme des relations multiplicatives créées, ce qui induit enfin une barrière de complexité naturelle en $L_q(1/3)$. Mais regardons de plus près qui sont ces groupes.

Moyenne et grande caractéristique : crible par corps de nombres. Les différentes variantes de cribles par corps de nombres se basent sur un diagramme qui part de l'anneau de polynômes à coefficients entiers $G_0 = \mathbb{Z}[X]$ et passe par deux corps de nombres $G_1 = \mathbb{Q}(X)/(f_1(X))$ et $G_2 = \mathbb{Q}(X)/(f_2(X))$. Les deux polynômes f_1 et f_2 sont choisis pour avoir une racine commune dans $\mathbb{F}_{p^n}$. La connaissance de G_1 et G_2 permet donc de retrouver G, c'est la représentation implicite que nous évoquions précédemment.

À l'intérieur de chaque corps de nombres, les petits éléments qui nous servent à construire la base de lissité sont les idéaux dont la norme est plus petite qu'une certaine borne de lissité. Le choix d'utiliser des idéaux vient du besoin d'obtenir une factorisation unique de chaque côté d'une relation. La manière de descendre explicitement ces idéaux vers le corps fini dans le diagramme est complexe, et nous en passerons les détails sous silence.

En compliquant encore, on peut utiliser un diagramme à plusieurs branches et tirer parti de l'utilisation de corps de nombres multiples. Cela a permis quelques avancées présentées cette année. En moyenne caractéristique, le crible par corps de nombres multiples [14] atteint une complexité asymptotique de $L_{p^n}(1/3, (8(9+4\sqrt{6})/15)^{1/3})$ tandis qu'en grande caractéristique le crible présenté dans [2] est de complexité $L_{p^n}(1/3, (2(46+13\sqrt{13})/27)^{1/3})$, cette seconde constante étant plus faible. De telles expressions peuvent sembler un peu barbares. Le second résultat est pourtant particulièrement intéressant puisque l'on retrouve exactement la complexité la plus basse connue pour factoriser un entier de même taille ! Et c'est plutôt heureux, car le crible par corps de nombres multiples est l'adaptation d'un algorithme de factorisation similaire.

Petite caractéristique : crible par corps de fonctions. En petite caractéristique, les groupes utilisés ont une structure plus simple puisqu'il s'agit de corps de fonctions. Depuis 2006, la simplification est telle que l'on ne considère plus que de simples anneaux de polynômes, bien que l'on conserve, par tradition, le terme de *crible par corps de fonctions*. Pour cette dernière construction, on a $G_0 = \mathbb{F}_p[X, Y]$, $G_1 = \mathbb{F}_p[X]$ et $G_2 = \mathbb{F}_p[Y]$, liés par des relations $Y = f_1(X)$ et $X = f_2(Y)$ permettant de définir les fonctions φ et ψ (par exemple $\psi_1(P(X, Y)) = P(X, f_1(X))$). La contrainte d'avoir une racine commune dans $\mathbb{F}_{p^n}$ s'exprime simplement en exigeant que $f_2(f_1(X)) - X$ ait un facteur irréductible de degré n.

Au lieu de chercher à factoriser des entiers (les normes des idéaux dans les corps de nombres), on travaille cette fois sur des polynômes à coefficients dans un petit sous-corps. Toutefois, la mécanique générale reste la même.

Cependant, la structure des polynômes sur des corps finis est bien mieux comprise ! Dans ce contexte, nous allons voir que l'un des ingrédients majeurs pour briser la barrière en $L_q(1/3)$ consiste à invalider l'heuristique usuelle en exhibant des polynômes de grands degrés , i.e., des éléments plus si petits que cela, qui ont la propriété agréable de se factoriser systématiquement en termes de petits degrés.

5. Du fracas en petite caractéristique

En 2013, plusieurs découvertes majeures ont profondément modifié la difficulté du problème du logarithme discret en petite caractéristique. Deux articles publiés en début d'année [10, 7] abaissent tout d'abord la deuxième constante de la complexité en $L_q(1/3, \cdot)$. La véritable rupture est la découverte [9] d'un algorithme en $L_q(1/4 + o(1))$. Ces trois articles travaillent essentiellement sur la façon de représenter le corps fini et de construire les relations multiplicatives. Quelques mois plus tard, une modification de la phase de descente du troisième algorithme conduit à un algorithme heuristique de complexité asymptotique[7] quasi-polynomiale [3].

Ces améliorations théoriques ont été couplées à de nouveaux et surprenants records de calculs : à l'heure actuelle, la cardinalité du plus gros corps fini dans lequel le problème du logarithme discret a été résolu s'écrit sur 9234 bits. Même s'il s'agit d'un corps un peu particulier, sa taille est dix fois supérieure au dernier record de 923 bits établi en 2012 avant ces avancées surprenantes.

7. Notons cependant que cette version de la descente n'est pas compétitive par rapport à la méthode en $L(1/4)$ pour les tailles actuelles des records de calcul.

5.1 – Représentation Frobeniale

Nous détaillons ici une version simplifiée de ces nouvelles méthodes, qui font appel à ce que l'on nomme la Représentation Frobeniale[8] (en opposition aux méthodes de crible). Cette version permet d'améliorer la complexité des deux premières phases. Elle reprend des travaux que nous avons menés récemment dans [11].

Les algorithmes par Représentation Frobeniale commencent par construire le corps fini $\mathbb{F}_{q^k}$ (où q n'est pas nécessairement premier) à l'aide d'un polynôme irréductible I de degré k tel que :

$$I(X) \quad \text{divise} \quad h_1(X)X^q - h_0(X)$$

où h_0 et h_1 sont deux polynômes de petits degrés. Si θ est une racine de I, on a ainsi choisi la représentation $\mathbb{F}_{q^k} = \mathbb{F}[\theta]$ de notre corps fini. En fait, comme il est facile de calculer explicitement les isomorphismes entre les différentes représentations de $\mathbb{F}_{q^k}$, ce choix n'est nullement une contrainte. De plus, il nous permet d'obtenir la relation $\theta^q = h_0(\theta)/h_1(\theta)$ dans le corps fini que l'on considère (d'où la notion de représentation par action de Frobenius). L'égalité absolument essentielle par la suite est l'identité polynomiale bien connue sur $\mathbb{F}_q[X]$:

$$\prod_{\alpha\in\mathbb{F}_q}(X-\alpha) = X^q - X.$$

En remplaçant X par $A(\theta)/B(\theta)$ pour A et B deux polynômes de degré au plus D et en multipliant par $B(\theta)^{q+1}$, on trouve dans le corps fini :

$$\begin{aligned} B(\theta)\prod_{\alpha\in\mathbb{F}_q}(A(\theta)-\alpha B(\theta)) &= A(\theta)^q B(\theta) - A(\theta)B(\theta)^q \\ &= A(\theta^q)B(\theta) - A(\theta)B(\theta^q) \end{aligned}$$

car $A(X)^q = A(X^q)$ par linéarité du Frobenius. On obtient finalement :

$$B(\theta)\prod_{\alpha\in\mathbb{F}_q}(A(\theta)-\alpha B(\theta)) = \frac{[A,B]_D(\theta)}{h_1(\theta)^D}, \qquad (2)$$

où $[A,B]_D$ désigne le polynôme de petit degré suivant :

$$h_1(\theta)^D\left(A\left(\frac{h_0(\theta)}{h_1(\theta)}\right)B(\theta) - A(\theta)B\left(\frac{h_0(\theta)}{h_1(\theta)}\right)\right).$$

Puisque les polynômes $A(\theta)-\alpha B(\theta)$ sont de degré au plus D, l'équation (2) donne une relation multiplicative entre polynômes en θ de degré au plus D pour une fraction constante des paires de polynômes (A,B). Comparativement aux algorithmes des générations précédentes, nous obtenons une relation dont nous ne testons la lissité que d'un seul côté (le côté gauche étant systématiquement lisse).

En utilisant ce principe avec des polynômes h_0 et h_1 bien choisis, il est possible de retrouver les logarithmes de tous les polynômes de degrés 2 en temps $O(q^5)$. Ceux-ci forment alors notre base de lissité initiale. Toutefois, cette base est trop petite pour directement permettre de s'intéresser à la phase de logarithmes individuels. Il est donc nécessaire de l'étendre pour lui adjoindre des polynômes de degrés plus élevés.

Pour cette extension, en regroupant astucieusement les éléments de la base étendue par paquets de polynômes *cousins* – par exemple, deux polynômes qui partagent le même coefficient constant sont cousins – on parvient à retrouver les logarithmes des polynômes de degrés 3 puis 4 en $O(q^6)$. Notons qu'il est bien plus efficace de procéder ainsi par extensions successives que de directement écrire des équations sur une base incluant tous les polynômes de degré 3, voire 4. En effet, ces approches directes amènent à des complexités bien moins bonnes en $O(q^7)$ ou même $O(q^9)$. Malgré tout, même avec ces complexités dégradées, le calcul initial des logarithmes des éléments de la base de lissité est polynomial en le logarithme de la cardinalité du corps considéré, ce qui est un énorme progrès par rapport aux algorithmes en $L(1/3)$ des générations précédentes.

5.2 – Logarithme individuel

Avec ce progrès sur la création des logarithmes de la base de lissité, on pourrait s'attendre à ce que l'ensemble du calcul de logarithme discret devienne polynomial. Mais ce n'est pas le cas, la phase finale permettant de calculer des logarithmes individuels, dont la contribution au coût du calcul était négligeable avec les anciennes méthodes, domine maintenant le coût asymptotique du calcul.

Sans se noyer dans les détails techniques, essayons de donner le principe général de la méthode. Pour trouver le logarithme d'un élément quelconque du corps fini $\mathbb{F}_{q^k}$, représenté par un polynôme $z(\theta)$ de degré au plus $k-1$, on cherche à

8. Il s'agit toujours de calcul d'indice, mais la première phase est modifiée en profondeur.

l'écrire comme produit (ou quotient) de polynômes de la base de lissité étendue (i.e. les polynômes de degré au plus 4). Comme on ne sait pas le faire directement, on procède par récurrence en cherchant à exprimer z comme produit (ou quotient) de polynômes de degré moitié au plus. Toutes ces expressions emboîtées peuvent se représenter par un arbre ayant z à sa racine et des polynômes de degré au plus 4 comme feuille. Dans cet arbre, chaque nœud a pour fils les polynômes de degrés plus petits qui servent à l'exprimer. Le nombre de nœuds de cet arbre correspond à la complexité du calcul du logarithme de z. Le degré étant divisé par 2 à chaque étage, la hauteur de l'arbre est une fonction logarithmique du degré de z, donc de k. Si le nombre de fils de chaque noeud pouvait être borné par une constante, la complexité serait polynomiale, mais nous allons voir que ce n'est pas le cas. En effet, pour créer des relations faisant intervenir z et capables de descendre jusqu'à la base de lissité, les méthodes connues nécessitent de réutiliser l'équation (2), cette fois avec des polynômes A et B de degrés plus élevés. Or, les équations de ce type contiennent au moins q termes, ce qui explique que la meilleure complexité atteignable par ce type de méthodes est de la forme $q^{O(\ln k)}$. Cette complexité est quasi-polynomiale dans la taille du corps $\ln q^k = k \ln q \approx q$ (puisque $k \approx q$).

En pratique, la situation est un peu plus complexe car on peut choisir de faire apparaître z soit à gauche, soit à droite dans l'équation (2). La première méthode découverte place z à droite et s'appuie sur la résolution d'équations bilinéaires dans les coefficients de A et de B pour construire ces polynômes, elle permet d'obtenir une complexité en $L(1/4)$. La seconde méthode consiste à placer z à gauche. D'un point de vue théorique, elle a permis d'atteindre une complexité quasi-polynomiale, toutefois, elle nécessite de calculer simultanément le logarithme de z et de q^2 polynômes cousins, ce qui la rend totalement inutilisable en pratique. Une troisième méthode [8] met de nouveau z à droite dans l'équation mais procède différemment pour reconstruire A et B, cela permet d'obtenir différemment une complexité quasi-polynomiale, tout en étant utilisable dans certains calculs pratiques.

5.3 – Conclusion

Malgré ces avancées récentes, le problème du logarithme discret reste d'une grande actualité. En petite caractéristique, l'espoir est de réussir à s'affranchir des diverses hypothèses heuristiques qui sous-tendent les méthodes actuelles. En pratique, ces résultats ont forcé l'abandon des algorithmes cryptographiques s'appuyant sur les corps finis de petite caractéristique, comme en témoignent les nouvelles recommandations de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) parues en 2013. Heureusement, la petite caractéristique étant assez peu utilisée pour des raisons historiques, cela n'a pas conduit à de trop lourdes conséquences.

Références

[1] L. M. Adleman. « A Subexponential Algorithm for the Discrete Logarithm Problem with Applications to Cryptography (Abstract) ». In : *FOCS*. 1979, p. 55–60.

[2] R. Barbulescu et C. Pierrot. « The multiple number field sieve for medium- and high-characteristic finite fields ». *LMS Journal of Computation and Mathematics* **17**, n° A (2014), p. 230–246. issn : 1461-1570.

[3] R. Barbulescu et al. « A Heuristic Quasi-Polynomial Algorithm for Discrete Logarithm in Finite Fields of Small Characteristic ». In : *EUROCRYPT*. 2014, p. 1–16.

[4] E. Canfield, P. Erdös et C. Pomerance. « On a problem of Oppenheim concerning factorisatio numerorum ». In : *Journal of Number Theory*. Vol. 17. 1983, p. 1–28.

[5] W. Diffie et M. E. Hellman. « New directions in cryptography ». *IEEE Transactions on Information Theory* **22**, n° 6 (1976), p. 644–654.

[6] T. E. Gamal. « A public key cryptosystem and a signature scheme based on discrete logarithms ». *IEEE Transactions on Information Theory* **31**, n° 4 (1985), p. 469–472.

[7] F. Göloglu et al. « On the Function Field Sieve and the Impact of Higher Splitting Probabilities - Application to Discrete Logarithms in $\mathbb{F}_{2^{1971}}$ and $\mathbb{F}_{2^{3164}}$ ». In : *CRYPTO (2)*. 2013, p. 109–128.

[8] R. Granger, T. Kleinjung et J. Zumbrägel. « On the Powers of 2 ». *IACR Cryptology ePrint Archive* **300** (2014).

[9] A. Joux. « A New Index Calculus Algorithm with Complexity $L(1/4 + o(1))$ in Small Characteristic ». In : *Selected Areas in Cryptography*. 2013, p. 355–379.

[10] A. Joux. « Faster Index Calculus for the Medium Prime Case Application to 1175-bit and 1425-bit Finite Fields ». In : *EUROCRYPT*. 2013, p. 177–193.

[11] A. Joux et C. Pierrot. « Improving the Polynomial time Precomputation of Frobenius Representation Discrete Logarithm Algorithms. A Simplified Setting for Small Characteristic Finite Fields ». In : *ASIACRYPT*. 2014.

[12] M. Kraïtchik. *Théorie des nombres*. Gauthier–Villars, 1922.

[13] D. Panario, X. Gourdon et P. Flajolet. « An Analytic Approach to Smooth Polynomials over Finite Fields ». In : *ANTS*. 1998, p. 226–236.

[14] C. Pierrot. « The Multiple Number Field Sieve with Conjugation and Generalized Joux-Lercier Methods ». *IACR Cryptology ePrint Archive* (2014).

[15] S. C. Pohlig et M. E. Hellman. « An improved algorithm for computing logarithms over GF(p) and its cryptographic significance (Corresp.) » *IEEE Transactions on Information Theory* **24**, n° 1 (1978), p. 106–110.

[16] J. Pollard. « Monte Carlo methods for index computations mod *p* ». In : *Mathematics of Computation*. Vol. 32. 143. 1978, p. 918–924.

[17] C. Pomerance. « Fast, rigorous factorization and discrete logarithm algorithms ». In : *Discrete algorithms and complexity*. Academic Press, 1987, p. 119–143.

[18] R. L. Rivest, A. Shamir et L. Adleman. « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems ». *Communications of the ACM* **21** (1978), p. 120–126.

[19] V. Shoup. « Lower Bounds for Discrete Logarithms and Related Problems ». In : *EUROCRYPT*. 1997, p. 256–266.

Antoine Joux

Chaire de cryptologie de la Fondation partenariale de l'UPMC, 4 place Jussieu, 75005 Paris, France et CryptoExperts, Paris, France

Antoine.Joux@m4x.org

Antoine Joux occupe la chaire de cryptologie de la fondation partenariale de l'UPMC (Paris 6). Il est également expert en sécurité chez CryptoExperts. Il a reçu le prix Gödel en 2013 pour l'introduction de la cryptographie reposant sur les couplages et se spécialise dans l'étude des problèmes algorithmiques utiles en cryptologie.

Cécile Pierrot

Laboratoire d'Informatique de Paris 6, UMPC, 4 place Jussieu, Paris, France et Direction Générale de l'Armement, Ministère de la Défense

Cecile.Pierrot@lip6.fr

Cécile Pierrot est en deuxième année de thèse à l'université Pierre et Marie Curie (Paris 6) sous la direction d'Antoine Joux. Son sujet d'étude est le problème du logarithme discret sur les corps finis et elle a publié plusieurs améliorations notables des algorithmes précédemment connus.

La conjecture de courbure bornée dans L^2 d'après les travaux de S. Klainerman, I. Rodnianski et J. Szeftel

• J. Smulevici

1. Introduction

La relativité générale est l'un des piliers de la physique théorique moderne. Une des grandes intuitions d'Einstein fut d'imaginer la gravitation non pas comme une force agissant sur une particule mais comme des contraintes géométriques. Lorsqu'une particule est soumise uniquement à la gravité, son inertie détermine sa trajectoire. Cette trajectoire n'est cependant pas forcément une ligne droite, la gravité déformant la géométrie. On peut penser par exemple à une bille roulant à l'intérieur d'un bol.

Mathématiquement, la géométrie est décrite par une variété, en général de dimension 4 (une dimension pour le temps, trois pour l'espace) munie d'une métrique lorentzienne. Contrairement aux métriques riemanniennes, qui sont définies positives, en géométrie lorentzienne, la longueur d'un vecteur peut être positive, négative, ou nulle.

Rappelons qu'en mécanique newtonienne, étant donné ρ la densité locale de matière, on détermine le potentiel gravitationnel en résolvant l'équation de Poisson

$$\sum_{i=1}^{3} \partial_{x^i}^2 \phi = \rho, \tag{1}$$

où $\phi : \mathbb{R}^3 \to \mathbb{R}$ est une fonction scalaire.

En relativité générale, la métrique lorentzienne joue le rôle du potentiel gravitationnel et l'équation de Poisson (1) est remplacée par un système d'équations aux dérivées partielles géométriques, qui fut proposé par Albert Einstein en 1915. Comme l'équation de Poisson, ces équations permettent de relier la gravitation, c'est-à-dire la géométrie, aux champs de matière. Par contre, contrairement à (1), les équations d'Einstein ont une dynamique très riche même en l'absence de toute source de matière. Ces équations, appelées alors *équations d'Einstein dans le vide*, s'écrivent

$$Ric(g) = 0, \tag{2}$$

où $Ric(g)$ désigne le tenseur de Ricci, un objet géométrique dépendant de la métrique g et de ses dérivées premières et secondes, dont la définition, ainsi que d'autres notions de géométrie lorentzienne seront rappelées au début de la section 2. Einstein lui-même avait déjà compris que les équations (2) décrivent des phénomènes de type ondulatoire et, en particulier, qu'il s'agit d'équations d'évolution. Le problème naturel est donc le problème de Cauchy, c'est-à-dire la construction, pour toutes données appropriées, d'une solution associée. Pour l'équation des ondes classique $\Box\phi = 0$ avec

$$\Box\phi := -\partial_t^2\phi + \sum_{i=1}^{3} \partial_{x^i}^2 \phi \tag{3}$$

l'opérateur des ondes, les données sur l'hypersurface $t = 0$ se composent d'un couple $\phi(t = 0)$ et $\partial_t\phi(t = 0)$. Dans le cas de (2), s'agissant d'une équation d'onde sur g, les données consistent en deux tenseurs symétriques d'ordre 2, (h, k), à partir desquels on peut reconstruire g et la dérivée normale de g sur une hypersurface.

Rappelons qu'on peut voir un tenseur d'ordre 2 sur une variété $\mathcal{M}$ comme une application de $\mathcal{M}$ à valeurs dans les formes bilinéaires sur l'espace tangent à $\mathcal{M}$ et dans le cas des tenseurs symétriques, à valeurs dans les formes bilinéaires symétriques.

Les données de Cauchy pour (2), formulées géométriquement, consistent alors précisément en un triplet (Σ, h, k) où (Σ, h) est une variété Riemannienne de dimension 3, k est un tenseur symétrique d'ordre 2 et les contraintes suivantes sont satisfaites

$$R^{(h)} - |k|^2 + (\mathrm{tr}\, k)^2 = 0, \tag{4}$$

$$\mathrm{div}^{(h)} k - \nabla^{(h)} \mathrm{tr}\, k = 0, \tag{5}$$

où $R^{(h)}$ est la courbure scalaire de h, $\nabla^{(h)}$ est la connexion de Levi-Civita associée à h, $\mathrm{div}^{(h)}k$ est la divergence de k pour la métrique h et $\mathrm{tr}^{(h)}k := \sum_{a,b} k_{ab}h^{ab}$ désigne la trace du tenseur k.

Une solution du problème aux données initiales associée à (Σ, h, k), appelée un développement des données, consiste en une variété lorentzienne $(\mathcal{M}, g)$ de dimension 4 et la donnée d'un plongement de Σ dans $\mathcal{M}$ tel que h corresponde à la métrique induite par g sur Σ et k corresponde à la deuxième forme fondamentale du plongement.

La conjecture de courbure bornée dans L^2, proposée initialement par Sergiu Klainerman en 1999 [6], affirme essentiellement que le problème aux données initiales pour les équations d'Einstein est bien posé dans la classe des données (Σ, h, k) telles que le tenseur de courbure de Riemann de h et les premières dérivées de k sont localement dans L^2. Puisque le tenseur de courbure dépend des dérivées secondes de la métrique et que k encode l'information sur la dérivée temporelle de la métrique, la conjecture correspond à un contrôle des solutions à l'aide seulement de bornes L^2 sur la métrique initiale et ses dérivées premières et secondes.

Cette conjecture a été finalement démontrée par Sergiu Klainerman, Igor Rodnianski et Jérémie Szeftel après des travaux s'étendant sur une dizaine d'années qui ont étés rendus publics en 2012 et 2013 dans les articles [9, 14, 15, 16, 17, 18].

La preuve de la conjecture de courbure bornée dans L^2 peut être vue comme le point d'orgue d'une longue série de travaux dédiés aux équations d'ondes quasi-linéaires à faible régularité appliqués à la relativité générale et à d'autres équations d'ondes géométriques. Ce domaine de recherche a une longue histoire, débutant avec les travaux pionniers de 1952 d'Yvonne Choquet-Bruhat établissant l'existence et l'unicité locale des solutions dans le cas régulier.

Dans le reste de cet article, nous essayerons, à défaut d'une présentation historique et exhaustive, d'introduire les éléments permettant de comprendre certaines caractéristiques importantes du problème et, en particulier, nous tenterons d'expliquer en quoi ce résultat est le premier de son genre.

2. Un peu de géométrie lorentzienne

Nous rappelons ici quelques définitions usuelles de géométrie lorentzienne qui seront utiles dans le reste du texte.

2.1 – Les bases

Définition 1. Une variété lorentzienne de dimension $3+1$ est une variété différentielle de dimension 4, notée ici $\mathcal{M}$, munie d'une métrique lorentzienne g, c'est-à-dire d'un 2-tenseur covariant de signature $(-+++)$.

La variété lorentzienne la plus simple, appelée *espace de Minkowski* ou espace plat, est la variété $\mathbb{R}^4$ munie de la métrique lorentzienne donnée globalement en coordonnées cartésiennes par $diag(-1,1,1,1)$.

Comme en géométrie riemannienne, on peut associer à toute métrique lorentzienne g , une connexion, notée ici D. La connexion D sert à généraliser la notion de dérivée aux tenseurs. Si X désigne un champ de vecteur, on note D_X la dérivée covariante dans la direction de X. Toute connexion doit vérifier

- pour les fonctions f : $D_X(f) = X(f) = \sum_\alpha X^\alpha \partial_{x^\alpha}(f)$;
- pour f une fonction et Y un champ de vecteur :

$$D_X(fY) = D_X(f).Y + fD_X(Y),$$

  avec $D_X(Y)$ un champ de vecteur ;
- pour k un tenseur d'ordre 2, Y et Z désignant des champs de vecteurs :

$$(D_X k)(Y,Z) = D_X(k(X,Y)) - k(D_X Y, Z) - k(Y, D_X Z),$$

  avec $D_X k$ un tenseur d'ordre 2.

Rappelons que si $(x^\alpha)_{\alpha=1,..,4}$ désigne un système de coordonnées sur $\mathcal{M}$, les dérivées partielles ∂_{x^α} peuvent être identifiées à des champs de vecteurs sur $\mathcal{M}$ et les dérivées covariantes D_α sont alors définies comme $D_\alpha := D_{\partial_{x^\alpha}}$.

Étant donnée une métrique g, on peut vérifier qu'il existe une unique connexion satisfaisant à $D_X g = 0$ pour tout champ de vecteur X, qui est appelée *connexion de Levi-Civita*. En coordonnée, pour un champ de vecteur X de composantes X^α, les composantes de ses dérivées covariantes sont données par

$$(D_\alpha X)^\beta = \partial_\alpha X^\beta + \sum_\gamma \Gamma^\beta_{\alpha\gamma} X^\gamma$$

où les coefficients $\Gamma^{\beta}_{\alpha\gamma}$, appelés *symboles de Christoffel*, sont calculables à l'aide des composantes de g et ses dérivées $\partial_{x^\alpha} g$.

En utilisant D, on peut définir le *tenseur de courbure de Riemann*, noté R. Pour tous champs de vecteurs X, Y, Z de la variété, on a par définition,

$$R(X,Y)[Z] = D_X D_Y Z - D_Y D_X Z - D_{[X,Y]} Z,$$

où $[X,Y] = \sum_\alpha [X,Y]^\alpha \partial_{x^\alpha}$ est le champ de vecteur de composantes

$$[X,Y]^\alpha = \sum_\beta X^\beta \partial_{x^\beta} Y^\alpha - Y^\beta \partial_{x^\beta} X^\alpha.$$

Les composantes du tenseur de courbure, notées $R^{\gamma}{}_{\rho\alpha\beta}$ (il s'agit d'un tenseur d'ordre 4), peuvent être calculées de la manière suivante. Pour tout champ de vecteur $X = \sum_\alpha X^\alpha \partial_{x^\alpha}$, nous avons

$$(D_\alpha D_\beta X)^\gamma - (D_\beta D_\alpha X)^\gamma = \sum_\rho R^{\gamma}{}_{\rho\alpha\beta} X^\rho.$$

R mesure donc essentiellement la non-commutativité des dérivées covariantes D_α.

À l'aide du tenseur de courbure, on construit le *tenseur de Ricci* apparaissant dans les équations d'Einstein (2).

Définition 2. Le tenseur de Ricci, $Ric(g)$, d'une métrique lorentzienne g est le tenseur symétrique d'ordre 2 dont les composantes dans un système quelconque de coordonnées sont données par

$$Ric(g)_{\alpha\beta} = \sum_\rho R^{\rho}{}_{\alpha\rho\beta}.$$

Le tenseur de Ricci est donc une trace partielle du tenseur de Riemann. Pour une métrique riemannienne, le tenseur de Ricci mesure la déviation (au second ordre) du volume d'une boule géodésique par rapport au volume euclidien correspondant. Une interprétation similaire peut être obtenue pour une métrique lorentzienne, en comparant la forme de volume écrite dans un système de coordonnées adaptées à des géodésiques (coordonnées normales) à la forme de volume de la métrique de Minkowski.

2.2 – Première et deuxième formes fondamentales

Rappelons aussi qu'étant donnée une hypersurface Σ, la métrique g induit sur Σ un 2-tenseur symétrique, noté ici h, appelé *première forme fondamentale* ou *métrique induite*. Σ est alors dite caractéristique (respectivement de type espace ou de type temps) si la signature de h est $(0,++)$ (respectivement $(+++)$ et $(-++)$). Étant donnée une hypersurface non-caractéristique, il existe, au signe près, une unique normale unitaire N définie sur Σ. La *deuxième forme fondamentale* de Σ est alors définie comme

$$k(X,Y) = -g(X, D_Y N),$$

où X et Y sont des champs de vecteurs tangents à Σ. On peut alors vérifier que k est un 2-tenseur symétrique.

2.3 – Feuilletages maximaux

Supposons que $(\mathcal{M}, g)$ puisse être feuilleté par les surfaces de niveau Σ_t d'une fonction de temps t, de telle sorte que $\mathcal{M} = \cup_t \Sigma_t$, avec Σ_t des hypersurfaces de type temps. Soit T la normale unitaire de Σ_t et h, k ses première et deuxième formes fondamentales. Le feuilletage est dit *maximal* si $\mathrm{tr}^{(h)}\mathrm{k} := \sum_{a,b} \mathrm{k}_{ab}\mathrm{h}^{ab} = 0$.

L'utilisation des feuilletages maximaux simplifie considérablement certains calculs. À titre d'exemple, le système des contraintes sur les données (4)-(5) se réduit à

$$\begin{aligned} R^{(h)} &= |k|^2, \\ \mathrm{div}^{(h)} k &= 0. \end{aligned}$$

2.4 – Géométrie lorentzienne globale

D'après la théorie de la relativité générale, la vitesse d'une particule ne peut pas dépasser la vitesse de la lumière. En géométrie lorentzienne, la trajectoire d'une telle particule correspond à une *courbe causale* dans notre variété, définie comme suit

Définition 3. Soient $(\mathcal{M}, g)$ une variété lorentzienne et γ une courbe régulière de $\mathcal{M}$, de vecteur tangent $\dot\gamma$. On dit que γ est une courbe causale si $g(\dot\gamma, \dot\gamma) \leqslant 0$ en tout point de la courbe.

Depuis les travaux de Jean Leray de 1952, on sait que pour une équation d'onde générale, la condition géométrique garantissant le domaine de dépendence des solutions (c'est-à-dire l'unicité) est la condition d'*hyperbolicité globale*. Dans le cadre de la géométrie lorentzienne, celle-ci est équivalente à la propriété suivante.

Définition 4. On dit d'une variété lorentzienne $(\mathcal{M}, g)$ qu'elle est globalement hyperbolique s'il existe une hypersurface Σ dans $\mathcal{M}$ telle que toute courbe causale intersecte Σ une et une seule fois.

Rappelons aussi la notion de variété asymptotiquement plate.

Définition 5. Soit (Σ, h, k) une donnée initiale pour les équations d'Einstein dans le vide. On dit que les données (h, k) sont asymptotiquement plates s'il existe un compact C dans Σ tel que $\Sigma \setminus C$ est difféomorphe à $\mathbb{R}^3 \setminus B(0,1)$ et si h converge vers la métrique euclidienne et k converge vers 0 à l'infini.

2.5 – Rayon volumique

En plus d'hypothèses sur la courbure et la deuxième forme fondamentale, les résultats mentionnés ci-dessous nécessitent aussi une hypothèse sur le rayon volumique, dont la définition est rappelée ici.

Définition 6. Soit (Σ, h) une variété riemannienne et $B_r(p)$ la boule géodésique de centre $p \in \Sigma$ et de rayon $r > 0$. Le rayon volumique en p aux échelles plus petites que r, noté $r_{vol}(p, r)$, est défini comme

$$r_{vol}(p, r) = \inf_{0<r'\leqslant r} \frac{|B_{r'}(p)|}{(r')^3},$$

où $|B_{r'}(p)|$ désigne le volume riemannien de $B_{r'}(p)$. Pour la variété Σ, on définit alors

$$r_{vol}(\Sigma, r) := \inf_{p\in\Sigma} r_{vol}(p, r).$$

Une borne inférieure sur le rayon volumique permet de découper notre variété en boules géodésiques sur chacune desquelles il sera plus facile d'estimer les solutions.

3. Les équations d'Einstein vues comme un système d'équations d'ondes quasi-linéaires

Nous rappelons ici quelques propriétés fondamentales des équations d'Einstein.

3.1 – Coordonnées d'ondes et première formulation comme un système d'équations d'ondes quasi-linéaires

Les équations (2) étant géométriques, un *choix de jauge*, par exemple le choix d'un système de coordonnées, est nécessaire pour transformer (2) en un système d'équations aux dérivées partielles. Une des jauges les plus fréquemment utilisées est le système de coordonnées d'onde (aussi appelé jauge harmonique en géométrie riemannienne). Dans la jauge d'onde, on considère un système de coordonnées $(x^\alpha)_{\alpha=1,..,4}$ sur une variété lorentzienne $(\mathcal{M}, g)$ tel que pour chaque α, x^α est solution de l'équation des ondes linéaires sur $(\mathcal{M}, g)$, i.e. $\Box_g x^\alpha = 0$, où $\Box_g$ est l'opérateur d'onde associé à g

$$\Box_g := \sum_{\alpha,\beta} g^{\alpha\beta} D_\alpha D_\beta,$$

où D désigne la connexion de Levi-Civita de g.

Dans cette jauge, les composantes de $Ric(g)$ se simplifient, de telle sorte que (2) se réduit à

$$\Box_g g_{\alpha\beta} = \mathcal{Q}_{\alpha\beta}(\partial g, \partial g), \qquad (6)$$

où $\mathcal{Q}_{\alpha\beta}(\partial g, \partial g)$ désigne une forme quadratique dans les premières dérivées de g avec des coefficients dépendant seulement de g.

Puisque le symbole principal de $\Box_g$, $\sum_{\alpha,\beta} g^{\alpha\beta}\xi_\alpha\xi_\beta$, est hyperbolique et dépend de la solution elle-même, le système ci-dessus est un système d'équations d'ondes quasi-linéaires.

3.2 – L'invariance d'échelle des équations

Notons que les équations sont invariantes par changement d'échelle : si g est une solution, pour tout $\lambda > 0$, la métrique définie en coordonnées par $(x^\alpha) \to g(\lambda x^\alpha)$ est aussi solution. Avec trois dimensions d'espace, l'espace de Sobolev $\dot{H}^s(\mathbb{R}^3) = \{f \in L^2(\mathbb{R}^3) / \int_{k\in\mathbb{R}^3} |k|^s |\mathcal{F}f(k)|^2\, dk < +\infty\}$, où $\mathcal{F}$ désigne la transformée de Fourier, reste invariant par cette transformation si $s = s_c = 3/2$ est *l'indice critique*. Les symétries d'échelle jouent un rôle important dans l'étude des équations d'ondes non-linéaires. Grossièrement, pour des régularités $s > s_c$, on peut diminuer la taille des données initiales tout en augmentant le temps d'existence des solutions tandis que pour $s < s_c$, on s'attend typiquement à ce que les équations soient mal posées.

3.3 – L'estimation d'énergie et la méthode classique

L'estimation fondamentale au centre de l'étude des équations (2) (ou de tout autre système d'équations d'ondes quasi-linéaires en dimension spatiale supérieure ou égale à deux) est l'estimation d'énergie. Dans le cas de l'équation des ondes classique

$\Box f = 0$, sur $\mathbb{R}_t \times \mathbb{R}^3_x$, on obtient (formellement) en multipliant l'équation par $\partial_t f$ et en intégrant par parties dans les variables d'espace, la conservation de l'énergie

$$\int_{\mathbb{R}^3} \left[(\partial_t f)^2(t) + \sum_{i=1,2,3} (\partial_{x^i} f)^2(t) \right] dx = \int_{\mathbb{R}^3} \left[(\partial_t f)^2(t_0) + \sum_{i=1,2,3} (\partial_{x^i} f)^2(t_0) \right] dx.$$

Pour (6), l'estimation d'énergie donne, pour tout $t \geqslant t_0$

$$\|\partial g(t)\|_{L^2_x} \lesssim \|\partial g(t_0)\|_{L^2_x} \exp\left(C \int_{t_0}^{t} \|\partial g(s)\|_{L^\infty_x} ds \right), \quad (7)$$

où t désigne une coordonnée de temps et $x = (x^1, x^2, x^3)$ désignent des coordonnées d'espace.

Pour exploiter cette estimation, on voit qu'on a besoin d'une borne uniforme sur

$$\int_{t_0}^{t} \|\partial g(s)\|_{L^\infty_x} ds. \quad (8)$$

La méthode à haute régularité consiste à estimer ∂g en norme L^∞ grâce au plongement de Sobolev $H^s(\mathbb{R}^n) \hookrightarrow L^\infty(\mathbb{R}^n)$, pour $s > n/2$. Par conséquent, avec 3 dimensions d'espace, la méthode classique pour des équations d'ondes quasi-linéaires telles que (6) nécessite que les données initiales pour g soient dans H^s avec $s > 5/2$. Elle conduit au théorème suivant.

Théorème 1 (Existence locale classique [4] et [10] pour l'unicité). *Soit (Σ, h, k) une donnée initiale pour les équations d'Einstein dans le vide (2). Supposons que Σ puisse être couverte localement par un nombre fini de systèmes de coordonnées formant une carte C^1, de telle sorte que $(h, k) \in H^s_{loc}(\Sigma) \times H^{s-1}_{loc}(\Sigma)$ avec $s > \frac{5}{2}$. Alors, on peut résoudre localement le problème de Cauchy associé à (Σ, h, k).*

Il existe de nombreuses motivations pour tenter d'améliorer les conditions de régularité dans le théorème ci-dessus. Une théorie bien posée pour des données à faible régularité implique typiquement un meilleur contrôle des solutions en temps long. Par exemple, l'étude des solutions à faible régularité permet de détecter la formation des singularités. Un autre d'exemple d'application concerne les théories bien posées dans des espaces *critiques*, c'est-à-dire en se rappelant la définition de la sous-section 3.2, dans des espaces de Sobolev H^s avec $s = s_c$. En effet, on peut typiquement transformer l'existence locale des solutions en existence globale pour des petites données. Finalement, il est souvent souhaitable d'obtenir un théorème d'existence locale dans un espace de données ayant une interprétation physique, comme l'espace des solutions d'énergie ou de masse finie, contrairement à un espace comme H^s avec $s > 5/2$ qui n'a a priori aucun lien avec la physique du problème.

3.4 – Estimations de Strichartz pour les équations d'ondes semi-linéaires et quasi-linéaires

Au vu de (7), l'obstruction principale pour fermer l'estimation d'énergie est déjà présente pour l'équation des ondes semi-linéaires

$$\Box \psi = \mathcal{Q}(\partial\psi, \partial\psi), \quad (9)$$

où $\Box$ désigne l'opérateur des ondes classique (3).

Pour abaisser la régularité nécessaire à l'étude d'équations telles que (9), on peut utiliser les estimations dites de *Strichartz*. Ces estimations permettent de contrôler les solutions des équations dans des espaces L^p avec $p > 2$, contrairement à l'inégalité d'énergie, à condition de *moyenner en temps* les estimations. Plus précisément, pour tout $\epsilon > 0$, les solutions suffisamment régulières de $\Box\phi = 0$ satisfont à

$$\left(\int_t \|\partial\phi(t,x)\|^2_{L^\infty_x} dt \right)^{1/2} := \|\partial\phi\|_{L^2_t L^\infty_x} \lesssim \|\phi(t=0)\|_{H^{2+\epsilon}_x} + \|\partial_t\phi(t=0)\|_{H^{1+\epsilon}_x}.$$

Nous voyons que l'estimation de Strichartz peut contrôler (8) avec moins de régularité car elle exploite l'intégrale en temps, contrairement à la méthode classique. Ceci conduit à une théorie bien posée pour (9) pour des données initiales dans $H^{2+\epsilon} \times H^{1+\epsilon}$ [11].

Dans le cas de l'équation quasi-linéaire (6), il y a plusieurs obstructions importantes au développement d'estimations de Strichartz. Au niveau linéaire, il s'agit de comprendre les estimations de Strichartz pour des équations d'ondes de la forme $\Box_g \psi = 0$, sous de faibles hypothèses de régularité pour la métrique g.

La première avancée sur cette question est venue avec les travaux de Bahouri-Chemin [1, 2], sui-

vis de travaux de Tataru [19, 20], dans lesquels ont été obtenues des estimations de Strichartz avec une petite perte de dérivée.

Les meilleurs résultats pour l'étude à faible régularité des équations d'onde quasi-linéaires à l'aide d'estimations de Strichartz ont été obtenus dans les travaux de Klainerman-Rodnianski [7] et Smith-Tataru [12]. Comparé aux travaux précédents mentionnés, ils utilisent l'observation importante que la métrique elle-même est solution des équations. Ceci a conduit à une théorie bien posée pour des données initiales dans $H^{2+\epsilon} \times H^{1+\epsilon}$, c'est-à-dire au même niveau de régularité que pour l'équation des ondes semi-linéaires (9).

3.5 – Estimations bilinéaires et la condition nulle

Étant donné que sans autre information sur la structure de la non-linéarité dans (9), il est connu, depuis des travaux de Hans Lindblad de 1993, que les résultats mentionnés précédemment sont optimaux, toute amélioration sur ces résultats doit exploiter certaines annulations dans (9) qui ne sont présentes que pour certains systèmes particuliers.

Dans [5], Klainerman et Machedon ont introduit un ensemble d'estimations, plus précisemment d'estimations bilinéaires, pour des non-linéarités satisfaisant à la *condition nulle*. Ce type de non-linéarité apparaît dans de nombreux systèmes d'équations issus de la physique, tels que les équations des applications d'onde, des champs de Yang-Mills ou encore celles du système de Maxwell-Klein-Gordon. Dans le cas des équations de Yang-Mills en dimension 3, les estimations bilinéaires de Klainerman et Machedon ont conduit à une théorie bien posée pour $s = s_c + 1/2$, où $s_c = 1/2$ est l'exposant critique de ces équations. L'importance de la condition nulle, identifiée initialement par Klainerman, a été à l'origine remarquée dans des travaux indépendants de Klainerman et Christodoulou de 1986 concernant l'existence globale à données petites pour des équations d'onde quasi-linéaires en dimension 3. Sous cette condition, les termes non-linéaires les plus dangereux peuvent tous être réécrits comme combinaisons linéaires des *formes nulles*

$$Q_0(\phi,\psi) = \partial_t\phi\,\partial_t\psi - \nabla\psi\cdot\nabla\phi, \qquad (10)$$
$$Q_{ij}(\phi,\psi) = \partial_i\phi\,\partial_j\psi - \partial_i\psi\,\partial_j\phi, \quad 1 \leqslant i,j \leqslant 3, \qquad (11)$$

où ϕ et ψ sont des composantes de la solution du système d'équations. À titre d'exemple, si ϕ et ψ sont des solutions suffisamment régulières de l'équation des ondes plate $\Box\phi = 0$, $\Box\psi = 0$, avec 3 dimensions d'espace on a l'estimation bilinéaire (linéaire en ψ et en ϕ) suivante :

$$\|Q_{ij}(\phi,\psi)\|_{L^2(\mathbb{R}_t\times\mathbb{R}^3_x)} \lesssim \|(\phi,\partial_t\phi(0)\|_{H^2(\mathbb{R}^3)\times H^1(\mathbb{R}^3)}\|(\psi,\partial_t\psi)(0)\|_{H^2(\mathbb{R}^3)\times H^1(\mathbb{R}^3)}.$$

À l'aide de cette estimation, on peut contrôler $Q_{ij}(\phi,\psi)$ en utilisant moins (plus précisément ϵ moins) de dérivées sur les données initiales que ce que permettent les estimées de Strichartz (et nettement moins de dérivées que ce que permettent les inégalités d'énergie). Dans le cas des équations de Yang-Mills en dimension 3, ce gain de régularité est crucial, car il permet de résoudre les équations localement dans l'espace d'énergie H^1. En effet, l'énergie étant conservée, on obtient immédiatement à partir de la théorie locale l'existence globale des solutions. De plus, l'énergie est une quantité physique, contrairement aux espaces $H^{1+\epsilon}$, donc on a une interprétation physique claire du résultat.

Implémenter un tel programme pour les équations d'Einstein comporte néanmoins de nombreuses difficultés, la première étant que les équations d'Einstein en coordonnées d'onde ne satisfont pas à la condition nulle, comme démontré par Y. Choquet-Bruhat dans [3].

3.6 – Stratégie pour une preuve de la conjecture de courbure bornée dans L^2

Au vu de la discussion ci-dessus, il y a deux étapes fondamentales qui semblent incontournables si l'on souhaite améliorer la théorie à faible régularité à l'aide de l'approche des estimations bilinéaires.

A- Trouver une nouvelle formulation des équations d'Einstein dans laquelle une version de la condition nulle est satisfaite.

B- Trouver une méthode appropriée pour obtenir les estimations bilinéaires pour les formes nulles apparaissant dans l'étape précédente.

De plus, toutes les preuves d'estimations bilinéaires (en dimension spatiale supérieure à 1) utilisent une représentation explicite des solutions, appelée *paramétrice*, afin d'obtenir l'étape *B*. Il semble donc nécessaire de

C- Construire une paramétrice Φ_F pour les solutions de l'équation de l'équation des ondes scalaires inhomogène $\Box_g \phi = F$, contrôler Φ_F ainsi que l'erreur $E = F - \Box_g \Phi_F$ (la paramétrice étant uniquement une solution approchée) et exploiter cette paramétrice pour obtenir les estimations bilinéaires désirées.

La preuve de plusieurs estimations bilinéaires de l'étape *B* se réduit en fait à la démonstration d'une estimation de Strichartz $L^4(\mathbb{R}_t \times \mathbb{R}^3)$ pour une version (localisée en fréquence) de la paramétrice de l'étape *C*. L'ingrédient final est donc

D- Démontrer une estimation de Strichartz $L^4(\mathbb{R}_t \times \mathbb{R}^3)$ pour une version localisée en fréquence de la paramétrice de l'étape C.

Finalement, mentionnons que :

– toutes les étapes précédentes doivent être implémentées en utilisant uniquement des bornes hypothétiques dans L^2 pour la courbure pour être cohérentes avec le résultat désiré.
– la preuve de chacune des étapes ci-dessus s'appuie sur les résultats des autres étapes, de telle sorte que plusieurs arguments de continuité sont nécessaires pour fermer toutes les estimations.

4. Le théorème de courbure bornée dans L^2

Les résultats principaux obtenus dans [9, 14, 15, 16, 17, 18] peuvent être résumés comme suit. [1]

Théorème 2. *Soit $(\mathcal{M}, g)$ un développement globalement hyperbolique de données initiales asymptotiquement plates pour les équations d'Einstein dans le vide (2). On suppose que $(\mathcal{M}, g)$ admet un feuilletage maximal par les surfaces de niveau Σ_t d'une fonction de temps t et que Σ_0 correspond à l'hypersurface initiale, la métrique induite étant notée h et la deuxième forme fondamentale étant notée k. On suppose de plus que*

$$Ric(h) \in L^2(\Sigma_0), \quad \nabla k \in L^2(\Sigma_0), \quad r_{vol}(\Sigma_0, 1) > 0,$$

où $r_{vol}(\Sigma_0, 1)$ est le rayon volumique aux échelles plus petites que 1. Alors, il existe un temps T ne dépendant que de $\|Ric(h)\|_{L^2(\Sigma_0)}$, $\|\nabla k\|_{L^2(\Sigma_0)}$ et $r_{vol}(\Sigma_0, 1)$ tel que les estimations suivantes sont vérifiées :

$$\begin{aligned} \|Riem(g)\|_{L^\infty[0,T]L^2(\Sigma_t)} &\leqslant C, \\ \|\nabla k\|_{L^\infty[0,T]L^2(\Sigma_t)} &\leqslant C, \\ \inf_{0 \leqslant t \leqslant T} r_{vol}(\Sigma_t, 1) &> 1/C, \end{aligned}$$

où $C > 0$ est une constante ne dépendant que de $\|Ric(h)\|_{L^2(\Sigma_0)}$, $\|\nabla k\|_{L^2(\Sigma_0)}$ et $r_{vol}(\Sigma_0, 1)$. En particulier, le temps d'existence d'une solution classique ne dépend que de $\|Ric(h)\|_{L^2(\Sigma_0)}$, $\|\nabla k\|_{L^2(\Sigma_0)}$ et $r_{vol}(\Sigma_0, 1)$.

Remarque 1. Le résultat ci-dessus a une interprétation physique claire, contrairement aux résultats précédents avec $g \in H^{2+\epsilon}$. En effet, la norme L^2 du tenseur de courbure sur une hypersurface donne une certaine mesure du flux d'énergie gravitationnel passant à travers cette hypersurface.

Remarque 2. Le résultat ci-dessus est le premier contenant des estimations à faible régularité pour des équations d'ondes quasi-linéaires pour lequel toute la structure des équations est importante et non pas uniquement la partie principale, comme c'était le cas dans les études à régularité $H^{2+\epsilon}$.

5. Quelques idées sur les élements de la preuve

5.1 – La condition nulle

Pour comprendre cette fameuse condition sur la structure de la non-linéarité, considérons d'abord une équation d'onde non-linéaire en dimension 1 d'espace

$$-\partial_t^2 \phi + \partial_x^2 \phi = \partial\phi\partial\phi,$$

où $\phi = \phi(t, x)$ et $\partial\phi\partial\phi$ désigne un produit quelconque de dérivées premières de ϕ.

Pour contrôler les solutions de cette équation, on peut essayer de démontrer une inégalité d'énergie. On peut facilement obtenir une estimation d'énergie si on a une borne $L^2(\mathbb{R}_t \times \mathbb{R}_x)$ sur la non-linéarité de la forme $\|\partial\phi\partial\phi\|_{L^2(\mathbb{R}_t \times \mathbb{R}_x)} \leqslant C$. Pour une non-linéarité quelconque, ceci correspond à une borne uniforme sur la norme L^4 de $\partial\phi$, qui n'est pas vérifiée si les données initiales pour $\partial\phi$ sont uniquement dans L^2.

Supposons maintenant que la non-linéarité ait une structure spéciale, plus spécifiquement qu'elle

1. Les articles mentionnés contiennent de nombreux autres résultats intermédiaires, que nous ne pouvons pas, faute de place, présenter ici. Outre les articles mentionnés, le lecteur intéressé pourra trouver dans [8] et [13] une présentation plus détaillée des résultats et de leurs preuves.

satisfasse à *la condition nulle*. En dimension 1 d'espace pour une équation scalaire, la condition nulle signifie simplement que le seul produit autorisé dans la non-linéarité est $\partial\phi\partial\phi = (\partial_t\phi + \partial_x\phi)(\partial_t\phi - \partial_x\phi)$. Pour comprendre pourquoi ce produit est meilleur qu'un produit quelconque, rappelons que si ϕ est solution de l'équation des ondes linéaires unidimensionelles $-\partial_t^2\phi + \partial_x^2\phi = 0$, alors ϕ peut s'écrire comme la somme de deux fonctions de la forme $\phi(t,x) = f(t+x) + g(t-x)$. Notons $u = t-x$ et $v = t+x$. On a alors $\partial_t + \partial_x = 2\partial_v$ et $\partial_t - \partial_x = 2\partial_u$ et donc

$$(\partial_t + \partial_x)\phi(t,x) = 2f'(v), \quad (\partial_t - \partial_x)\phi(t,x) = 2g'(u),$$

de telle sorte que

$$\begin{aligned}
&\|(\partial_t\phi + \partial_x\phi)(\partial_t\phi - \partial_x\phi)\|^2_{L^2(\mathbb{R}_t\times\mathbb{R}_x)} \\
&= \int_t\int_x (\partial_t\phi + \partial_x\phi)^2(\partial_t\phi - \partial_x\phi)^2\,dxdt \\
&= 8\int_u\int_v (f'(v))^2(g'(u))^2\,dudv \\
&= 8\left(\int_u (g'(u))^2\,du\right).\left(\int_v (f'(v))^2\,dv\right), \\
&\lesssim \|\partial\phi(t_0)\|^4_{L^2(\mathbb{R})},
\end{aligned}$$

où $\partial\phi(t_0)$ désigne les données initiales pour $\partial\phi$. À l'aide de cette inégalité, on peut alors facilement montrer que pour cette non-linéarité, le problème est bien posé dans H^1, ce qui est mieux que la régularité optimale pour une non-linéarité quelconque. Dans la preuve de la conjecture de la courbure L^2, un des éléments clés de la preuve est donc de mettre en évidence *une structure nulle* des termes non-linéaires.

5.2 – La paramétrice de J. Szeftel

Dans la sous-section précédente, pour démontrer l'estimation

$$\|(\partial_t\phi + \partial_x\phi)(\partial_t\phi - \partial_x\phi)\|^2_{L^2(\mathbb{R}_t\times\mathbb{R}_x)} \lesssim \|\partial\phi(t_0)\|^4_{L^2(\mathbb{R})},$$

nous avons utilisé une *représentation explicite des solutions* puisque nous avons réécrit $\phi(t,x)$ comme la somme $f(t+x) + g(t-x)$.

Pour l'équation des ondes classiques en trois dimensions, on peut de manière analogue démontrer des estimations pour les formes nulles en utilisant une représentation explicite des solutions, en utilisant la transformée de Fourier. Plus précisément, si f est une solution suffisamment régulière de l'équation des ondes plate $\Box f = 0$ alors on a

$$f(t,x) = \int_{\lambda\in\mathbb{R}_+}\int_{\omega\in\mathbb{S}^2} \left[e^{i\lambda(t+\omega.x)}f_1(\lambda\omega) + e^{i\lambda(t-\omega.x)}f_2(\lambda\omega)\right]\lambda^2\,d\lambda\,d\omega,$$

où les fonctions f_1 et f_2 sont obtenues à l'aide des transformées de Fourier des données initiales $f(0,x)$ et $\partial_t f(0,x)$. Les phases $t \pm \omega.x$ sont liées à la géométrie du problème. En effet, en notant $u_\pm(t,x,\omega) = t \pm \omega.x$, on a $g(\nabla u_\pm, \nabla u_\pm) = 0$ si g est la métrique plate de Minkowski introduite au début de la sous-section 2.1.

Dans ses travaux, J. Szeftel a introduit une représentation explicite des solutions de $\Box_g\phi = 0$, où g est maintenant une métrique faiblement régulière, similaire à la paramétrice ci-dessus. Pour tenir compte de la géométrie, les phases $t \pm \omega.x$ sont maintenant remplacées par des solutions de l'équation $g(\nabla u, \nabla u) = 0$, appelée *équation eiconale*, où g est une métrique lorentzienne faiblement régulière. Contrairement à la métrique plate, la paramétrice est seulement une solution approchée et les phases ne sont pas connues explicitement. Une part importante de la preuve consiste donc à construire et contrôler les phases et estimer de manière appropriée l'erreur, alors qu'on ne contrôle que faiblement g.

5.3 – Les équations d'Einstein comme un système de Yang-Mills quasi-linéaire

Comme expliqué ci-dessus, une des étapes clés de la preuve consiste à déterminer une formulation des équations d'Einstein pour laquelle la condition nulle est vérifiée.

La nouvelle formulation adoptée, et dans laquelle la condition nulle est vérifiée, est une formulation de type *Yang-Mills*. Celle-ci repose sur la méthode des repères mobiles d'Élie Cartan. Elle consiste à décomposer les tenseurs, non pas sur des bases de champs de vecteurs (∂_{x^α}) associées à un système de coordonnées $(x^\alpha)_{\alpha=0,..,3}$, mais à l'aide d'une base de champs de vecteurs orthonormée (e_α). Dans le contexte lorentzien, « base orthornormée » signifie $g(e_\alpha, e_\beta) = diag(-1,1,1,1)$.Si on considère maintenant un système de coordonnées locales $(x^\mu)_{\mu=0,..,3}$, nous pouvons définir une 1-forme à valeurs dans les matrices anti-symétriques par $\sum_\mu A_\mu dx^\mu = \sum_\mu g(D_\mu e_\beta, e_\alpha)dx^\mu$. Le cœur de la formulation de Yang-Mills des équations d'Einstein consiste alors à réécrire les équations comme un

système d'équations sur les composantes de A, au lieu d'un système d'équations sur les composantes de g. Pour faire apparaître les formes nulles, l'argument principal suit des idées développées par Ulhenbeck en 1982 pour l'étude de systèmes elliptiques. Les équations sur A sont valides pour toute base orthonormée (e_α) et en choisissant convenablement la base orthonormée, de manière similaire à l'introduction de la jauge de Coulomb en théorie de l'électromagnétisme, on peut alors faire en sorte que les termes non-linéaires dans les équations pour A sont tous, soit des formes nulles de type (11), soit des termes d'ordre supérieur facilement contrôlables.

Références

[1] H. Bahouri et J.-Y. Chemin. « Équations d'ondes quasilinéaires et effet dispersif ». *Internat. Math. Res. Notices*, n° 21 (1999), p. 1141–1178.

[2] H. Bahouri et J.-Y. Chemin. « Équations d'ondes quasilinéaires et estimations de Strichartz ». *Amer. J. Math.* **121**, n° 6 (1999), p. 1337–1377.

[3] Y. Choquet-Bruhat. « The null condition and asymptotic expansions for the Einstein equations ». *Ann. Phys. (8)* **9**, n° 3-5 (2000). Journées Relativistes 99 (Weimar), p. 258–266.

[4] T. J. R. Hughes, T. Kato et J. E. Marsden. « Well-posed quasi-linear second-order hyperbolic systems with applications to nonlinear elastodynamics and general relativity ». *Arch. Rational Mech. Anal.* **63**, n° 3 (1976), 273–294 (1977). ISSN : 0003-9527.

[5] S. Klainerman et M. Machedon. « Space-time estimates for null forms and the local existence theorem ». *Comm. Pure Appl. Math.* **46**, n° 9 (1993), p. 1221–1268.

[6] S. Klainerman. « PDE as a unified subject ». *Geom. Funct. Anal.* n° Special Volume, Part I (2000). GAFA 2000 (Tel Aviv, 1999), p. 279–315.

[7] S. Klainerman et I. Rodnianski. « Rough solutions of the Einstein-vacuum equations ». *Ann. of Math. (2)* **161**, n° 3 (2005), p. 1143–1193.

[8] S. Klainerman, I. Rodnianski et J. Szeftel. « Overview of the proof of the Bounded L2 Curvature Conjecture ». *1204.1772* (2013).

[9] S. Klainerman, I. Rodnianski et J. Szeftel. « The Bounded L2 Curvature Conjecture (Accepté pour publication dans Invent. Math.) » *arXiv :1204.1767* (2012).

[10] F. Planchon et I. Rodnianski. « Uniqueness in Relativity ». *Preprint, See also* Chruściel P. T., Galloway G. and Pollack D., Mathematical general relativity : a sampler, *Bull. Amer. Math. Soc.* **47**, n° 4 (2010).

[11] G. Ponce et T. C. Sideris. « Local regularity of nonlinear wave equations in three space dimensions ». *Comm. Partial Differential Equations* **18**, n° 1-2 (1993), p. 169–177.

[12] H. F. Smith et D. Tataru. « Sharp local well-posedness results for the nonlinear wave equation ». *Ann. of Math. (2)* **162**, n° 1 (2005), p. 291–366.

[13] J. Smulevici. « d'après S. Klainerman, I. Rodnianski et J. Szeftel, Bourbaki seminar on the bounded L^2 curvature conjecture ». *Institut Henri Poincaré* (juin 2014).

[14] J. Szeftel. « Parametrix for wave equations on a rough background I : regularity of the phase at initial time ». *arXiv :1204.1768* (2012).

[15] J. Szeftel. « Parametrix for wave equations on a rough background II : construction and control at initial time ». *arXiv :1204.1769* (2012).

[16] J. Szeftel. « Parametrix for wave equations on a rough background III : space-time regularity of the phase ». *arXiv :1204.1770* (2012).

[17] J. Szeftel. « Parametrix for wave equations on a rough background IV : control of the error term ». *arXiv :1204.1771* (2012).

[18] J. Szeftel. « Sharp Strichartz estimates for the wave equation on a rough background ». *arXiv :1301.0112* (2013).

[19] D. Tataru. « Strichartz estimates for operators with nonsmooth coefficients and the nonlinear wave equation ». *Amer. J. Math.* **122**, n° 2 (2000), p. 349–376.

[20] D. Tataru. « Strichartz estimates for second order hyperbolic operators with nonsmooth coefficients. III ». *J. Amer. Math. Soc.* **15**, n° 2 (2002), 419–442 (electronic).

Jacques Smulevici

Laboratoire de mathématiques, université Paris-Sud, bât. 425, 91405 Orsay, France

jacques.smulevici@math.u-psud.fr

Les maths vues par un artiste : une expérience de diffusion de la culture mathématique via l'art et l'histoire de l'art

- S. Vinatier
- R. Alcorn

Le projet *Convergences*, mené conjointement par l'Institut de recherche sur l'enseignement des mathématiques (IREM) de Limoges, l'artiste Reg Alcorn et le CCSTI [1] du Limousin *Récréasciences*, explore les liens entre mathématiques et art de deux manières. Au cœur du projet il y a l'idée que l'art peut être un moyen original et puissant de diffusion de la culture mathématique auprès du grand public et des scolaires. En utilisant des créations artistiques pour parler de mathématiques nous espérons susciter la curiosité de ces publics et les affranchir du cadre scolaire auquel ils associent souvent cette discipline, leur permettant ainsi de lire ou d'entendre les explications scientifiques associées aux tableaux, en l'occurrence, avec un regard neuf. Par ailleurs, une partie du projet consiste à évoquer l'influence des mathématiques dans les développements artistiques de quelques époques clefs, ce qui permet d'introduire de façon très variée les contenus proposés : à travers les mathématiques bien sûr, mais aussi l'art, l'histoire, l'histoire de l'art et l'histoire des mathématiques. On espère toucher ainsi des publics très divers ; par la même occasion on met en avant les liens entre les mathématiques et le monde réel : constructions, représentations, évolutions dans la façon d'appréhender le monde.

À l'origine du projet il y a l'intérêt de l'artiste Reg Alcorn d'abord pour les sciences, en particulier la chimie des pigments, puis pour les mathématiques : les célébrations du centième anniversaire du décès de Poincaré en 2012 l'ont amené à se pencher sur l'histoire de cette discipline et à établir des ponts avec l'histoire des arts : « L'histoire des mathématiques mérite d'être mieux connue, avec les personnalités intrigantes et géniales comme Euler, Gauss, Poincaré, Hilbert ou Mandelbrot ; la diversité des langages mathématiques ; le sens de la poésie et de la beauté. De plus, ce qui m'intrigue et ne peut me laisser indifférent, c'est l'intérêt des enfants pour la peinture ; et ceci, malgré la sophistication des images de synthèse et de modélisation. Il me semble qu'il est possible d'avoir une cohabitation entre l'image créée et la pensée abstraite ».

1. Thèmes scientifiques

Cette curiosité a fait écho à l'intérêt de l'IREM de Limoges pour la diffusion de la culture mathématique et scientifique. S'est ensuivi un long travail commun, fait de discussions, réflexions et lectures, auquel ont pris part de nombreux animateurs IREM et enseignants chercheurs du Département Mathématiques et Informatique du laboratoire XLIM [2] pour dégager les thèmes que nous étions susceptibles de développer. Nous les avons regroupés en deux expositions à destination du grand public et des scolaires :

– l'exposition *Poincaré – Turing (1854-1912-1954)* rend hommage à Henri Poincaré et Alan Turing, à l'occasion du centenaire du décès du premier et de la naissance du second, en présentant une partie de leur œuvre scientifique ; en plus d'éléments biographiques pour les deux savants, on y aborde la classification des surfaces, la stabilité du système solaire,

1. Centre de culture scientifique technique et industrielle.
2. UMR 7252 CNRS – Université de Limoges.

le disque de Poincaré, la machine de Turing, la cryptanalyse d'Enigma et la morphogenèse et on y présente deux animations informatiques : le Jeu de la Vie et l'agrégation limitée par diffusion ;
– l'exposition *Convergences : les mathématiques dans l'histoire de l'art* se propose d'exhiber quelques liens entre les mathématiques et l'histoire de l'art en se focalisant sur quatre périodes historiques : l'Antiquité avec le nombre d'or dans l'architecture et la sculpture ainsi que les gammes pythagoriciennes, le Moyen Âge avec les pavages en pays d'Islam, la Renaissance avec l'invention de la perspective, enfin le xx^{e} siècle avec l'abstraction et l'art numérique ; elle est accompagnée d'un perspectographe et de jeux de pavages de Penrose.

L'originalité de ces expositions est double. D'une part elles confrontent des panneaux expliquant les notions mathématiques et des tableaux de l'artiste, créations originales ou copies de tableaux classiques (même si, dans l'exposition *Convergences*, la correspondance entre les tableaux et les panneaux n'est pas complètement achevée : les trois tableaux proposés par l'artiste pour le xx^{e} siècle appellent un panneau décrivant notamment le mouvement conjoint vers l'abstraction de l'art et des mathématiques du début de cette période, tandis que les panneaux de la période Antique n'ont pas été illustrés par des tableaux).

D'autre part elles ont bénéficié de compétences locales spécifiques. Il s'agit notamment d'un groupe de l'IREM de Limoges qui a travaillé en 2010 - 2012 sur l'enseignement de la perspective dans le cadre des programmes de mathématiques du collège [3] (une brochure de l'IREM de Limoges est en préparation) ; d'un autre groupe qui a réfléchi en 2011 - 2014 sur l'introduction d'une approche historique dans l'enseignement des mathématiques au collège [4] et a fait travailler des élèves de 6^{e} sur le découpage des carrés à la façon d'Abū l-Wafā', ce qui a donné lieu à un article dans la revue du réseau des IREM [5]. Le responsable de ce groupe, Marc Moyon, est maître de conférences en histoire des mathématiques à l'ESPE de l'académie de Limoges ; il a apporté au projet ses connaissances de spécialiste des mathématiques médiévales en pays d'Islam. Benoît Crespin, maître de conférences en synthèse d'images au sein du Département Mathématiques et Informatique du laboratoire XLIM s'est chargé des animations et panneaux liés à l'informatique, en particulier de celui sur les images de synthèse (en lien avec l'art du xx^{e} siècle). D'autres collègues enfin ont apporté leurs compétences en musique, chimie, cryptographie, histoire, français, ou encore construction de jeux mathématiques.

2. Aiguiser la curiosité des visiteurs

FIGURE 1 – *Portrait d'Henri Poincaré* (1,7× 1,5 m, des équations plein la tête) et *Portrait d'Alan Turing* (1,5× 1,14 m), Reg Alcorn, 2012.

En plus des dix panneaux explicatifs et de deux animations informatiques, l'exposition *Poincaré–Turing (1854-1912-1954)* est composée de quatre toiles grand format très spectaculaires : pour chacun des deux savants, un portrait réalisé d'après

3. http://www.irem.unilim.fr/recherche/archives/la-perspective-a-la-renaissance/
4. http://www.irem.unilim.fr/recherche/archives/histoire-des-mathematiques-au-college/
5. M. Moyon, Diviser en multipliant les approches… Quand les mathématiques remontent aux sources, *Repères IREM*, **93**, 2013.

photo et évoquant ses activités scientifiques et un tableau illustrant certains de ses travaux. La taille, la composition, les couleurs des tableaux donnent un attrait indéniable à l'exposition ; le regard de l'artiste sur les thèmes traités assure qu'ils le sont de façon accessible : sans formation scientifique, il se met naturellement à la portée du plus grand nombre, sans pour autant édulcorer le message. Ses difficultés en tant qu'« outsider » contribuent ainsi à une certaine justesse dans la vulgarisation et constituent une arme plutôt qu'un désavantage.

Ainsi le tableau consacré à la classification des surfaces et à l'effet papillon, intitulé *Le petit déjeuner de Poincaré*, représente de façon très réaliste les formes géométriques couramment évoquées dans les livres de mathématiques : beignets, bretzels, tasses... complétées par quelques autres ingrédients d'un petit déjeuner.

Figure 2 – *Le petit déjeuner de Poincaré* (2,2× 1,5 m), Reg Alcorn, 2012.

Toutes ces formes flottent dans l'air en désordre, offrant une entrée ludique qui permet de parler de classification des surfaces dès l'école primaire (comment mettre de l'ordre dans ce bazar ? en comptant le nombre de trous !), à charge pour le visiteur d'approfondir le message en se reportant aux deux panneaux liés au tableau ou, en cas de visite commentée, à l'animateur d'adapter son discours à l'auditoire. On peut aller jusqu'à évoquer les grandes lignes de la conjecture de Poincaré et même prétendre, en extrapolant sans doute les intentions de l'artiste, que les objets sont suspendus en vol pour représenter la dimension temporelle (ils ne peuvent rester ainsi en l'air qu'un instant) laquelle, ajoutée aux trois dimensions spatiales de la scène représentée en perspective, nous montre l'espace de dimension quatre où cette conjecture se place. C'est la force de l'artiste, nourri par le dialogue avec le scientifique, que de pouvoir représenter quatre dimensions sur une toile qui n'en possède en réalité que deux !

L'exposition *Convergences : les mathématiques dans l'histoire de l'art* reprend ce principe avec des toiles plus petites mais en plus grand nombre : une dizaine de tableaux représentant des pavages (créations ou copies de mosaïques), six tableaux inspirés de la Renaissance italienne (Paolo Uccello, Piero della Francesca, Raffaello, Leonardo da Vinci), trois tableaux pour évoquer l'art du xx^{e} siècle (des copies d'Albers et Picasso et une création à la Pollock). Là encore les tableaux attirent le regard et aiguisent la curiosité des visiteurs, tout en permettant d'introduire des notions mathématiques plus ou moins sophistiquées en fonction du public : proportions, polygones, symétries, périodicité, parallèles, lignes de fuite... Des jeux de pavages de Penrose poursuivent le même but : une entrée ludique vers un contenu réellement mathématique ; un perspectographe rudimentaire complète l'expérience. Avec toujours la possibilité d'approfondir la visite en consultant les onze panneaux explicatifs, voire en complétant les activités du livret d'accompagnement (niveau CM1 - CM2 - 6^{e}).

Figure 3 – Quelques tableaux de l'exposition *Convergences*, Reg Alcorn, 2013.

3. Divers lieux d'exposition

Les deux expositions *Poincaré - Turing* et *Convergences* ont déjà été présentées un grand nombre de fois dans toute la région Limousin et au delà. Quelques milliers d'élèves de fin de primaire ou du secondaire les ont visitées. Après la Fête de la Science 2012 et quelques sites universitaires à Limoges, la première est partie au lycée Jean Baptiste Darnet de Saint Yrieix la Perche, à la médiathèque intercommunale de Haute-Corrèze à Ussel, puis au lycée Pierre Bourdan à Guéret. La seconde a d'abord été présentée lors de la Fête de la Science 2013 à Limoges, puis au collège Fernand Lagrange à Pierre-Buffière, à l'ESPE de l'académie de Limoges, au salon des Jeux Mathématiques à Paris (partiellement), à la bibliothèque municipale et dans la salle de conférences de Saint Léonard de Noblat, à la Maison des Jeunes et de la Culture de La Baule, au collège René Bernier de Saint Sébastien sur Loire, au collège Pierre de Ronsard et à la cité scolaire Léonard Limosin à Limoges.

On le voit, les lieux d'accueil sont variés, ils dépendent essentiellement des contacts établis avec les divers acteurs de la diffusion de la culture scientifique (enseignants, bibliothécaires, associations,...) ; dans certains cas, ces acteurs nous contactent parce qu'ils sont en demande de contenus liés à la manifestation qu'ils organisent, sans connaître l'exposition au préalable, dans d'autres cas ils l'ont vue ou en ont entendu parler (voire ont participé à sa réalisation) et souhaitent la faire venir au plus près de leur public.

4. Divers publics

Ces publics sont variés eux aussi : quelques présentations sont destinées au grand public, en particulier lors de la fête de la science (à Limoges on accueille essentiellement les scolaires en semaine et le grand public le week-end). On propose alors des visites en accès libres ou commentées par un scientifique, par l'artiste Reg Alcorn ou par les deux.

La plupart des présentations sont tournées aussi, voire majoritairement, vers les scolaires, pour lesquels on organise des visites commentées, le plus souvent couplées à un atelier (par exemple sur les pavages), ce qui permet de dédoubler les groupes. À chaque fois, les classes de CM1 et CM2 se sont montrées très intéressées par cette formule, mise en place avec l'aide du *Point Sciences*[6] de la DSDEN[7] de la Haute-Vienne. Ces visites sont assez souvent l'occasion de liaisons primaire - collège (le mélange d'élèves des différents niveaux conduit souvent à des accès de timidité ou de fanfaronnerie en début de séance). On les couple parfois aussi avec une séance animée par un enseignant ou par un atelier de dessin animé par l'artiste.

Figure 4 – Divers publics pour les expositions *Poincaré - Turing* et *Convergences*

Hormis les 6e dans le cadre des liaisons, les classes du secondaire ont réservé un accueil variable à nos expositions. Quelques expériences avec diverses classes de lycée ont été tout à fait satisfaisantes, voire enthousiasmantes : ce fut le cas notamment avec des classes de seconde de Brive, de La Baule et de Limoges visitant l'exposition *Convergences*, ainsi qu'avec une classe de terminale d'Ussel visitant l'exposition *Poincaré - Turing* avec son professeur de philosophie. Comme bien souvent, il semble que l'implication du professeur accompagnateur, pendant la présentation ou en amont, qu'il soit mathématicien ou non, soit déterminante pour que les élèves s'investissent dans la visite et en tirent un profit maximal. Les classes de 4e et 3e sont les plus difficiles à faire adhérer au projet. Si l'on

6. Centre départemental de ressources pour l'enseignement scientifique et technologique, `http://pointsciences.iahautevienne.ac-limoges.fr/`.

7. Direction des Services Départementaux de l'Éducation Nationale.

se laisse aller à donner une explication assez répandue sans être en mesure de l'étayer, on pourrait dire que la curiosité des années antérieures s'est un peu émoussée et que les capacités de concentration, peut-être moins développées qu'au lycée, sont déjà très sollicitées par les enseignements scolaires. Une expérience de visite commentée par l'artiste les pinceaux à la main a montré qu'il est tout de même possible de capter ce public. Une autre piste pourrait être d'inscrire la visite de l'exposition *Convergences* dans la préparation de l'épreuve d'histoire de l'art du brevet des collèges, à condition de trouver des enseignants motivés pour faire travailler leurs élèves sur des thèmes en lien avec l'exposition.

5. Événements organisés en lien avec les expositions

La plupart des présentations des expositions sont accompagnées d'événements destinés à attiser la curiosité des publics visés et enrichir leur expérience. Au delà du traditionnel vernissage ou des visites commentées déjà évoquées, il peut s'agir de conférences tout public, données par des spécialistes et permettant d'approfondir un des thèmes traités dans l'exposition, par exemple *Quelques aspects de la vie et de l'œuvre du mathématicien Henri Poincaré* par Gilles Godefroy (Paris), *Astronomie et mathématiques* par Alex Esbelin (Clermont-Ferrand), *Quand les plantes font des maths* par Anne-Marie Aebischer (Besançon), *Lorsque les Mathématiques et les Arts se rencontrent : l'exemple des pays d'Islam* par Marc Moyon (Limoges), *La perspective décomposée* par Denis Favennec (Bordeaux), *Cristallographie et symétrie* par Bernard Maitte (Lille).

Il peut s'agir aussi, en phase avec le versant artistique du projet et en lien avec ses thèmes scientifiques, de performances artistiques. Deux sortes de performances ont été proposées jusqu'alors. La plus originale, avec une seule occurrence, consiste en une confrontation artiste / informaticien en images de synthèse : tous deux doivent représenter en parallèle un objet donné, chacun avec ses moyens, toile – pinceaux – peinture pour l'un, scanner 3D – ordinateur – logiciels de retouche d'image pour l'autre. Proposée lors de la Fête de la Science 2013, elle a dû se faire sans scanner 3D pour cause de panne, en utilisant un modèle numérique disponible de l'objet à représenter, ce qui a quelque peu réduit le temps de travail de l'informaticien aux commandes. L'intérêt de la performance a été préservé grâce à un de ses collègues qui a commenté au micro les techniques utilisées et fait apparaître les points communs (plus nombreux qu'on pourrait penser !) et les différences avec celles de l'artiste. L'idée de ce match homme / machine était apparue pendant les conversations préparatoires du projet.

Figure 5 – Tableau du spectacle *Le Chant des cristaux*, Reg Alcorn, 2014.

L'autre performance a été conçue par l'artiste Reg Alcorn, à l'origine du projet, en collaboration avec le clavieriste Paul Fenton. Les deux artistes avaient déjà expérimenté la peinture en direct et en musique à quelques reprises. Ils ont repris cette formule en l'adaptant à des thèmes liés aux expositions : *Réaction-diffusion* (Turing a montré que ce type de réaction chimique pouvait intervenir dans certains processus de morphogenèse), *Quadrivium* (astronomie, arithmétique, géométrie et musique, les quatre « arts mathématiques » de l'Antiquité et du Moyen Âge), *Le Chant des cristaux* (en lien avec les pavages), chacun donnant lieu à une toile et une partition originales. Celles-ci sont composées et répétées à l'avance, refaites en direct lors de la performance, suivies de quelques explications de la part du peintre. L'originalité du spectacle proposé (on voit rarement un artiste peindre en direct, *a fortiori* sur des thèmes scientifiques, *a fortiori* mathématiques), ainsi que sa qualité artistique, sont garantes de son succès devant de très nombreux publics.

6. Financement

On ne peut clore ce compte-rendu d'expérience sans évoquer la question cruciale du financement. Dès le départ il a semblé souhaitable que l'exposition soit prêtée gratuitement aux institutions qui voudraient la présenter et que, dans la mesure du possible, l'IREM de Limoges aide à sa mise en valeur dans les différents lieux (transport, installation, visites, conférences...). Cela impliquait de rassembler à l'avance des financements suffisants pour couvrir

la conception et la réalisation de l'exposition, en particulier les tableaux, ainsi qu'au moins une partie de son fonctionnement. Le contexte actuel d'économies tous azimut n'était pas très prometteur, pourtant le projet a bénéficié d'un soutien conséquent de l'université de Limoges (pour environ les 2/3 du budget total, tous services confondus : services centraux, IREM, Mission *Diffusion Savoirs et Culture*, laboratoire XLIM, Fondation Partenariale). Notre partenaire le CCSTI *Récréasciences* a bien sûr participé aux dépenses, ainsi que la ville de Limoges et quelques sponsors privés (MAIF, MGEN et CASDEN) qui se sont laissés convaincre assez facilement. Le consortium de diffusion de la culture mathématique Cap'Maths a accepté de participer au budget de l'exposition à hauteur de 7% des dépenses, sous la forme d'une subvention versée à l'issue de l'opération sur présentation des pièces justificatives. La somme reçue s'ajoute au reliquat de budget et permet d'envisager le financement d'autres actions pour continuer à faire vivre l'exposition.

7. Perspectives

Parmi ces actions, en plus de la présentation des expositions dans de nouveaux lieux ou à de nouveaux publics, on aimerait compléter l'exposition *Convergences* par des tableaux pour le module *Antiquité* et des panneaux pour le module *xx*^{e} *siècle*. On projette aussi, vaste chantier, de rédiger et d'éditer un catalogue commenté de cette exposition. Notons que le Département Mathématique et Informatique du laboratoire XLIM a repris le principe du projet *Convergences* : il a fait appel à l'artiste Reg Alcorn pour réaliser des tableaux qui évoquent ses thèmes de recherche, avec l'IREM de Limoges dans le rôle d'entremetteur entre l'artiste et les scientifiques. Accrochés dans les couloirs bordant les bureaux des chercheurs, ils permettent d'organiser des visites guidées du département à destination du grand public et des scolaires. Les premières visites effectuées ont montré une nouvelle fois le grand pouvoir d'attraction des toiles de l'artiste et leur potentiel pour diffuser la culture mathématique et informatique.

Figure 6 – *Reproduction d'une mosaïque d'Uccello à la Basilique Saint Marc à Venise*, Reg Alcorn, 2013.

Stéphane Vinatier

IREM de Limoges, 123 avenue Albert Thomas, 87060 Limoges cedex - http://www.irem.unilim.fr
stephane.vinatier@unilim.fr

Stéphane Vinatier est maître de conférences. Au sein de l'institut XLIM (UMR CNRS 7252), il étudie certaines structures galoisiennes en théorie algébrique des nombres. Directeur de l'IREM, il s'occupe notamment de diffusion de la culture mathématique, en particulier en animant des visites commentées pour les scolaires des expositions réalisées avec Reg Alcorn.

Reg Alcorn

http://www.regalcorn-artscience.fr et http://www.histoireenpeinture.fr

William Reginald Alcorn est né en 1950 en Zambie de parents irlandais et écossais. Une passion pour la peinture se révèle très tôt. Après des études dans les humanités en Angleterre, il voyage en Europe, pour se fixer en France. Avec les projets engagés dans la musique, les langues, les sciences et récemment les mathématiques, il divise son temps entre son atelier de peintre et les animations de vulgarisation, notamment dans le cadre des activités de l'IREM de Limoges.

Une bonne trentaine de personnes se sont impliquées, de près ou de loin et à divers titres, dans la réalisation et l'animation des deux expositions. Nous tenons à les remercier pour leur engagement dans ce projet, ainsi bien sûr que nos soutiens financiers cités plus haut. Parmi elles, nous remercions plus particulièrement : Elisabeth Alcorn, Cédric Alves, Emmanuel Blancher, Sophie Couteaud, Benoît Crespin, Marie Doneda, Pierre Dusart, Paul Fenton, Pierre Fournier, Martine Guerletin, Michel Métrot, Marc Moyon et Stéphane Reyrolle.
Pages web consacrées au projet : http://www.irem.unilim.fr/les-maths-vues-par-un-artiste/

Les filières scientifiques d'excellence : un imprenable bastion masculin ?

• A. PIERREL

Cet article s'appuie sur une recherche de sociologie menée à l'initiative de l'École normale supérieure de Paris sur les biais – aussi bien en termes de genre que d'origines sociales – dans le recrutement des filières scientifiques de l'établissement [1]. Étant entendu que tout ne se joue pas au moment des concours d'entrée, mais que ceux-ci parachèvent un processus de sélection entamé bien en amont dans les trajectoires scolaires, nous avons cherché à rendre compte des différents seuils (d'orientation ou de sélection) de la disparition graduelle des filles et des élèves d'origines populaires. Un relevé des proportions de filles aux différentes étapes menant vers la rue d'Ulm confirme ce caractère graduel : les filles représentent 45% des élèves de Terminale S, 26% des effectifs des classes MPSI et PCSI (mais 70% des BCPST), 25% des MP* et PC*, 20% des inscrits aux concours MP, Info et PC de l'ÉNS Paris, 9% des admissibles et des admis à ces trois concours. Il convient de se garder de tirer des conclusions trop hâtives de cette diminution progressive de la proportion de filles, car elle n'est que le reflet d'une pluralité de logiques articulées entre elles. Parle-t-on toujours des mêmes filles (et corrélativement des mêmes garçons) à mesure que l'on avance dans le processus de sélection scolaire ? Comment départir les effets de celui-ci des choix d'orientation, en prenant en compte le fait que ces derniers intègrent de manière plus ou moins consciente les probabilités objectives de réussite et que « s'autoriser à y croire » n'est pas uniquement le fait de volontés individuelles mais se construit par tout un ensemble d'incitations émanant aussi bien du milieu familial d'origine que de l'institution scolaire ? Tenter d'éclaircir ces quelques questions n'a pas pour objectif premier de livrer une explication « clés en mains » de la disparition graduelle des filles des filières scientifiques d'excellence (et moins encore de formuler des moyens d'y pallier), mais plutôt d'esquisser un cadre pour poser adéquatement cette question. Dans cette perspective, nous allons développer successivement quatre points dont la prise en compte permet de se prémunir contre quelques fausses pistes d'explication.

1. Les orientations post-baccalauréat : un espace complexe

La structuration sexuée de l'espace de l'enseignement supérieur est un fait bien connu : aux filles, les filières littéraires, juridiques, de sciences humaines ; aux garçons, les filières scientifiques et techniques. Cette partition renvoie en partie à un principe de différenciation sexuée très général entre le « monde des choses humaines » dévolu aux femmes et le « monde des choses matérielles » aux hommes, dont la pertinence a été éprouvée à propos d'autres domaines de pratiques [2]. Cependant cette partition est loin d'être suffisante. En effet, les filles sont loin d'être absentes de toutes les filières scientifiques de l'enseignement supérieur et y sont même majoritaires dans nombre d'entre elles, telles que la biologie, la chimie ou encore la médecine. Autrement dit, la structuration sexuée se rejoue au sein des filières scientifiques et existent des sciences au masculin et des sciences au féminin.

1. Marianne Blanchard, Sophie Orange, Arnaud Pierrel, *La production d'une noblesse scientifique : enquête sur les biais de recrutement à l'ÉNS*, 2014.

2. Par exemple à propos des pratiques de lectures masculines et féminines, voir Claude Fossé-Poliak, Gérard Mauger, Bernard Pudal, *Histoires de lecteurs*, Editions du Croquant, 2010 [1999].

L'exemple de la médecine montre également que le caractère sexué d'une filière n'est pas « gravé dans le marbre » : alors que les filles constituaient un tiers des effectifs au début des années 1970, elles en représentent aujourd'hui plus des deux tiers.

Il faut se garder d'expliquer ces répartitions différenciées entre filières uniquement à l'aune de supposés goûts ou dégoûts disciplinaires et ce pour deux types de raisons. Premièrement, les appellations de filières ne traduisent pas forcément l'intégralité des disciplines qui y sont enseignées et existent à ce titre des « matheuses invisibles ». C'est par exemple le cas des classes préparatoires aux écoles de commerce où les mathématiques constituent l'enseignement principal en termes de volume horaire et dont le coefficient aux épreuves des concours est le plus élevé pour les écoles les plus prestigieuses (HEC, ESSEC). Or, à l'aune des résultats d'admission à ces écoles de commerce, les filles y réussissent aussi bien que les garçons et la féminisation de ces établissements, à partir des années 1970 est allée de pair avec leur légitimation au sein de l'enseignement supérieur [3]. Deuxièmement, les orientations féminines vers les filières scientifiques ne traduisent pas nécessairement des passions pour telle ou telle discipline et qui seraient vécues comme une transgression des stéréotypes de sexe, mais peuvent procéder d'autres déterminations. C'est ce qu'invite à penser l'un des entretiens que nous avons menés avec une jeune fille en PCSI d'un grand lycée parisien. Voici comment relate-t-elle « son choix » d'orientation :

> Même si à un moment on a pensé m'inscrire en fac de droit, donc c'était pas du tout l'idée de départ la PC, je n'avais pas d'idée finalement au départ. [...] Parce que mon frère il a fait ça, c'était évident [*elle souligne*] qu'il ferait ça. Tout le monde savait qu'il ferait une prépa scientifique. Pour moi, c'était un peu « elle peut aussi partir dans une école de commerce », ça aurait pu vraiment être autre chose. [...] Dans la famille, les gens ont fait soit médecine, soit une prépa [scientifique]. Donc de toute façon, je ne connaissais pas d'autres voies. C'est pour ça que, finalement, on a été assez réticents à m'envoyer dans un truc comme fac de droit ou tout ça, parce qu'on ne connaît pas.

Dans l'ombre de la vocation scientifique du frère aîné (elle mentionne, au cours de l'entretien, qu'elle l' « admire » et que « tout le monde [lui] dit qu'[elle] parle trop de [s]on frère »), sa propre orientation vers une classe préparatoire scientifique ne s'apparente pas à une transgression des stéréotypes de sexe, mais à un choix, parmi d'autres possibles et familialement concerté, d'études respectables.

2. La classe sociale des lettres, le genre des sciences ?

Les différences d'orientation et de réussite scolaire ont, historiquement, d'abord été appréhendées au prisme des milieux sociaux d'origine des élèves. La proximité de la culture bourgeoise et de la culture scolaire est, dans cette perspective, au fondement des inégalités scolaires et la dissimulation de cette proximité permet de recouvrir les inégalités d'un voile méritocratique [4]. De prime abord, la culture scientifique semble être à l'abri de ce phénomène en tant que son contenu relève de la pure logique, et donc ne serait pas plus en affinité avec un milieu social plutôt qu'un autre. Pour autant, ce caractère logique de la culture scientifique n'empêche pas qu'elle fasse l'objet de transmissions familiales, très inégalement réparties selon les milieux sociaux. Dans le questionnaire que nous avons diffusé auprès d'étudiants en classes préparatoires scientifiques (N = 2345), nous demandions à ceux-ci s'ils étaient aidés dans leur travail scolaire par l'un des membres de leur famille. Les proportions de réponse affirmative s'échelonnent selon les milieux sociaux d'origine : 47% des étudiants dont le père est ingénieur ou professeur ont répondu positivement, contre 30% de ceux dont le père appartient aux autre catégories supérieures (cadres du public, du privé, professions libérales) et 16% des étudiants issus des catégories moyennes ou populaires. Les transmissions familiales de la culture scientifique ne prennent pas seulement la forme d'un adjuvant au travail scolaire, mais ce faisant, elles participent aussi à l'intériorisation d'une certaine aisance vis-à-vis des objets mathématiques. C'est ce que donne à voir l'entretien réalisé avec

3. Voir Marianne Blanchard, « Quand féminisation rime avec légitimation », *Histoire de l'éducation*, n° 136, 2012.
4. C'est là la substance des analyses de Pierre Bourdieu et Jean-Claude Passeron dans *Les héritiers*, Éditions de Minuit, 1964 et *La reproduction*, Éditions de Minuit, 1970.

Alix [5], majore de sa classe de MPSI d'un grand lycée parisien et dont le travail scolaire est encadré de près (avance sur le programme pendant les vacances d'été, correction d'exercices, etc.) par son père enseignant-chercheur en mathématiques et son grand-frère normalien, également en mathématiques. Cet entretien met en évidence que l'aisance mathématique se caractérise par une certaine *manière de voir* [6], un rapport réflexif aux contenus enseignés qui permet de donner du sens à chacune des parties en tissant des liens avec le tout. Ce goût des mathématiques comme manière de voir ne se dit jamais aussi bien que lorsqu'il est comparé aux aspects calculatoires de la discipline, comme l'atteste ce passage de l'entretien :

> - Et dans les différentes compétences mathématiques à avoir, entre ce qui est calculatoire et ce qui fait appel à l'intuition, toi c'est quoi que tu maîtrises le mieux, qu'est-ce que tu préfères ?
>
> - Alors, je préfère et je crois maîtriser mieux le côté où on visualise les choses, on voit les choses, on sent les choses. Je déteste [*elle souligne*] le côté calculatoire. Typiquement, en physique et en sciences de l'ingénieur, les calculs qui s'alourdissent, ça me fait suer, c'est horrible ! C'est juste parce que quand on calcule, ce qui m'énerve beaucoup, c'est qu'au fond, ce n'est pas difficile. Enfin, personnellement, je ne pense pas que ce soit difficile. On peut toujours bien mener un calcul. Si tu me donnes assez de temps, je pourrais finir bien le calcul. Par contre, il n'est pas vrai que si tu me donnes assez de temps, je comprendrais cette théorie. Je ne pense pas que ce soit le même niveau de difficulté, et il y a beaucoup de gens qui pensent qu'être fort, c'est être très rapide en calcul.

Le calcul est ainsi renvoyé du côté de la pure technique, qui ne demande pas de facultés intellectuelles particulières (« On peut toujours bien mener un calcul »), voire, métaphoriquement, d'un labeur physique (susceptible de « s'alourdir » ou de « faire suer »), par opposition à la théorie, affaire de qualités abstraites (« voir », « sentir les choses »). Que les transmissions familiales ne soient pas l'apanage de la culture lettrée, mais qu'elles opèrent aussi pour la culture scientifique nous conduit à formuler trois brèves remarques. Premièrement, étant donné les inégales possibilités de transmissions familiales selon les milieux sociaux, aborder la question du recrutement des filières scientifiques d'excellence uniquement au prisme des différences filles/garçons s'avère insuffisant : il convient d'articuler systématiquement les inégalités sexuées aux inégalités d'origines sociales. Deuxièmement, que l'aisance mathématique (« visualiser les choses ») puisse être le fruit d'un fort investissement familial dans la discipline invite à ne pas rabattre d'emblée – à la fois conceptuellement et *pédagogiquement* – la capacité d'intuition sur des dispositions innées, mais à considérer aussi que cette intuition peut faire l'objet d'apprentissages. Troisièmement, l'analyse statistique des variations de la proportion de filles en fonction des configurations familiales des étudiants (études et professions des parents et aîné-e-s de la fratrie) corrobore l'importance des transmissions par les lignées maternelles pour que se forme et se réalise un projet d'études scientifiques chez les jeunes filles [7]. Si, globalement, la proportion de filles dans les effectifs de MP et PC augmente significativement lorsque l'un des deux parents est ingénieur (32% contre 26% pour la situation contraire), l'effet est bien plus marqué lorsqu'il s'agit des mères (39%, quelle que soit la profession des pères) que lorsque ce sont les pères qui sont ingénieurs (31% de filles, quelle que soit la profession des mères).

3. « S'autoriser à y croire » : une construction collective

Les filles seraient sous-représentées dans les filières scientifiques d'excellence parce qu'elles « n'oseraient pas » s'y engager et, pour les étudiantes de CPGE, tenter leurs chances aux concours réputés les plus difficiles. Répandue, cette explication psychologisante par « l'auto-censure » confine à la tautologie dès lors que sont occultés les processus sociaux de la construction de la croyance en sa propre valeur scolaire. Plusieurs travaux ont déjà mis en évidence que, dans l'enseignement secondaire, la dynamique des interactions entre enseignants et élèves, dans les cours de mathématiques, est à l'avantage des garçons. Notam-

5. Le prénom est anonymisé.
6. Voir également Muriel Darmon, *Classes préparatoires, la fabrique d'une jeunesse dominante*, Éditions La Découverte, 2013.
7. Résultat déjà mis en évidence par Catherine Marry, *Les femmes ingénieurs. Une révolution respectueuse*, Belin, 2004. Voir notamment la partie intitulée « Héritages et transmissions maternelles », pp. 141-160.

ment, les prestations de ceux-ci ont tendance à être perçues comme la marque d'un talent personnel au moindre coût scolaire, tandis que les filles redoubleraient d'efforts pour faire du mieux qu'elles peuvent [8]. Cette économie de la perception professorale (largement inconsciente) différenciée selon le sexe des élèves est susceptible de puissants effets de retour sur l'autoperception des élèves de leur valeur scolaire et ce dès le collège. En effet, lorsque les filles obtiennent des notes en mathématiques supérieures à la médiane au contrôle continu du brevet des collèges, elles sont 83% à s'attribuer un « assez bon » ou un « très bon » niveau, alors que c'est le cas de 89% des garçons. Plus encore, seulement 53% des garçons ayant obtenu des notes inférieures à la médiane admettent avoir « de grosses » ou « un peu de difficultés », contre 71% des filles. Plus incités à croire dans leurs compétences mathématiques, les garçons reconnaissent ainsi, le cas échéant, moins souvent que les filles leurs difficultés en la matière. Ce marquage différencié de la valeur scolaire mathématiques des filles et garçons perdure au fil des trajectoires. Dans le cadre de notre recherche sur les CPGE scientifiques, nous avons suivi une promotion d'élèves (n = 176, soit deux classes MPSI-MP et deux de PCSI-PC) au prisme de leurs quatre, ou six (pour les 5/2), bulletins scolaires semestriels, en relevant systématiquement les types d'appréciations qui y figuraient. Le constat est sans appel : alors même que filles et garçons réussissent en première année aussi bien les uns que les autres (ce qu'objectivent des passages en classe étoile en 3/2 dans les mêmes proportions), les jugements professoraux diffèrent. Aux filles, le « sérieux » ; aux garçons, le « potentiel » ou les « capacités inexploitées ». Le lien entre ces jugements différenciés et la construction de la croyance en sa valeur scolaire est lui aussi patent : ceux dont le « potentiel » est souligné à trois reprises ou plus dans les bulletins semestriels tentent leur chance au concours de l'ÉNS proportionnellement trois fois plus souvent que les autres (*ie.* deux occurrences ou moins) [9]. De sorte que les filles, pourtant aussi souvent que les garçons dans les classes étoiles de ce lycée, sont sous-représentées parmi ceux qui ont passé le concours de l'ÉNS. Ce n'est là qu'une facette du caractère collectif de la construction de la croyance en sa valeur scolaire. Il conviendrait de souligner également le rôle des milieux sociaux d'origine, en premier lieu parce qu'ils conditionnent le type d'établissement fréquenté en CPGE, qui structure fortement l'horizon des écoles jugées atteignables « et donc valant la peine d'en passer les concours d'entrée » par les étudiants.

4. « Filles », « garçons » : de qui parle-t-on ?

Les réflexions uniquement focalisées sur la question des stéréotypes sociaux de sexe attachés aux disciplines ou filières tendent implicitement à homogénéiser les groupes en présence, « filles » d'un côté et « garçons » de l'autre. Or, au fil du processus de sélection scolaire menant jusqu'à la réussite au concours d'entrée de l'ÉNS (ou de toute autre grande école très sélective), ces groupes se modifient doublement et la prise en compte de ces changements morphologiques est indispensable pour rendre compte des différents filtres de sélection. Premièrement, si les filles sont *in fine* très largement sous-représentées parmi les admis aux concours scientifiques de la rue d'Ulm, toutes ne sont pas évincées au même moment. L'enquête par questionnaire auprès des élèves des CPGE montre que la sélection qui s'opère au moment du passage en deuxième année par la répartition des étudiants entre classes « étoiles » et « non-étoiles » se fait au détriment des filles d'origines sociales moyennes ou populaires. En revanche, leurs camarades d'origines supérieures sont aussi fréquemment présentes dans les classes « étoiles » que les garçons issus des mêmes catégories sociales. S'agissant du concours de l'ÉNS [10], ce sont trois variables qu'il faut articuler entre elles pour rendre compte de la variation des taux de réussite : le sexe des candidats, leur milieu social d'origine et le type d'établissement qu'ils ont fréquenté en CPGE. Du côté des filles inscrites au concours de l'ÉNS, seules celles cumulant les avantages d'une origine sociale supérieure et de la fréquentation d'un grand lycée parisien présentent un taux de réussite (2,9%) qui ne fait pas figure d'exception statistique. Du côté des garçons, la structure est étagée

8. Pour un exemple parmi d'autres, voir Isabelle Collet, « Les filles toujours fâchées avec les sciences ? », *Cahiers pédagogiques*, nº 476. `www.cahiers-pedagogiques.com/Les-filles-toujours-fachees-avec-les-sciences`.

9. Bien entendu, le fait d'être inscrit au concours de l'ÉNS ne figure pas dans les bulletins. Nous avons construit cette variable par recoupement des noms des élèves de cet établissement avec les bases des inscrits au concours que l'ÉNS a mises à notre disposition.

10. Nos analyses couvrent la période 2008-2013, années pour lesquelles l'École nous a transmis les bases de données sur les inscrits aux concours d'entrée (n = 15 508).

en trois groupes : en ordre décroissant, ceux d'origine supérieure des grands lycées parisiens (7,8%) / ceux d'origine moyenne ou populaire (3,8%) de ces mêmes établissements et ceux d'origine supérieure des grands lycées de province (4,1%) / les garçons d'origine moyenne ou populaire des grands lycées de province (2,7%). S'il convient ainsi d'articuler sexe et origines sociales pour rendre compte du processus de sélection scolaire, il faut aussi souligner que les caractéristiques des individus que l'on regroupe sous une même appellation (« filles d'origines populaires », « garçons d'origines supérieures », etc.) changent au long du processus de sélection : le substantif ne fait pas substance. Ce second point est essentiel pour comprendre qu'au moment des concours ce sont ceux qui sont les plus représentés parmi les inscrits qui y réussissent le mieux (autrement dit, dont la part augmente encore au fil des étapes du concours), à savoir les garçons d'origines supérieures. En effet, ce ne sont pas ces deux attributs en eux-mêmes qui font la réussite aux concours et ce n'est qu'une « minorité des meilleurs » d'entre eux (comme des autres sous-groupes) qui sont au final déclarés admis. Mais, étant les plus nombreux parmi les inscrits et ceux dont la croyance dans leur valeur mathématique a été la plus entretenue tout au long de leur parcours scolaire, c'est dans ce sous-groupe qu'il y a le plus de chances de trouver certains individus possédant la combinaison de caractéristiques rares d'excellence scolaire qui permet de franchir avec succès la barrière très sélective du concours d'entrée.

Rendre compte de la sous-représentation des filles dans les filières scientifiques d'excellence appelle ainsi plusieurs précautions méthodologiques et requiert de se garder d'explications « toutes faites » trop hâtives. S'agissant des mathématiques en particulier, soulignons deux points susceptibles de faire, un tant soit peu, bouger les choses. Premièrement, donner à voir les incontestables réussites des « matheuses invisibles » dans les filières qui ne sont pas explicitement classées comme études scientifiques pourrait avoir comme vertu certains effets de retour sur les aspirations de leurs cadettes et l'autoperception que ces dernières ont de leur valeur scolaire en mathématiques. Deuxièmement, l'analyse des transmissions familiales de la culture scientifique invite à casser l'idée encore bien ancrée d'un « fatalisme de l'intuition » – qualité que l'on posséderait ou non et ce irrémédiablement – pour affirmer avec force et auprès de tous les publics que faire des maths… ça s'apprend ! En termes de pratiques pédagogiques, débouter ce « fatalisme de l'intuition » passe, entre autres, par une explicitation attentive des notions mathématiques étudiées, sans présumer par exemple de la « trivialité », aux yeux de tous les élèves, de certains raisonnements. On peut à cet égard se demander si le témoignage, datant de 1974, de Michèle Vergne à propos de ses années à l'ÉNS de Fontenay ne comporte pas encore une part de vérité lorsqu'elle déclarait : « Comme c'était la mode, les professeurs passaient très vite sur les détails fastidieux des démonstrations et que moi, je ne voyais pas à quels objets connus, classiques, elles renvoyaient, je ne pouvais pas rétablir les jalons qui manquaient… "Par un raisonnement standard, on prouve que"… et je me sentais réduite à l'infériorité totale de ne pas pouvoir deviner quel était ce raisonnement standard [11] ».

Arnaud Pierrel
Arnaud Pierrel, est agrégé de sciences économiques et sociales et doctorant en sociologie au Groupe de Recherches et d'Études Sociologiques du Centre Ouest (Gresco) à Poitiers.

11. Michèle Vergne, « Témoignage d'une mathématicienne », *in* Pierre Samuel (sld.), *Mathématiques, mathématiciens et société*, Publications mathématiques d'Orsay, n° 86 74-16, 1974. Disponible en ligne, `http://sites.mathdoc.fr/PMO/afficher_notice.php?id=PMO_1974_A19`

… le processus SLE

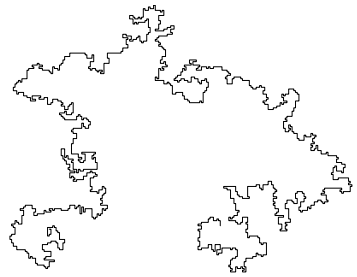
• V. BEFFARA

Soit n un entier positif : une *marche auto-évitante* de longueur n sur le réseau $\mathbb{Z}^2$ est un chemin discret $(x_i)_{0\leqslant i\leqslant n}$ issu de $x_0 = 0$, tel que x_i et x_{i+1} soient voisins pour tout i, et tel que les x_i soient tous distincts. L'ensemble Ω_n des marches auto-évitantes de longueur n est fini, et il est facile de montrer par un argument de sous-multiplicativité que son cardinal c_n satisfait à

$$\frac{1}{n}\ln c_n \xrightarrow[n\to\infty]{} \ln \mu$$

avec $\mu \in (2,3)$, appelé *constante de connectivité* de $\mathbb{Z}^2$. C'est à peu près tout ce qu'on sait des marches auto-évitantes en dimension 2 ! En particulier on ne connaît pas la valeur exacte de μ.

FIGURE 1 – Une longue marche auto-évitante.



Les conjectures ne manquent pas. La plus facile à énoncer concerne toujours c_n : les physiciens prédisent que

$$c_n = \mu^n n^{11/32+o(1)}.$$

Le comportement d'une longue marche auto-évitante « typique » (tirée au sort uniformément dans Ω_n avec n grand) reste également mystérieux : on conjecture que l'extrémité fluctue plus que celle d'une marche aléatoire simple, et que

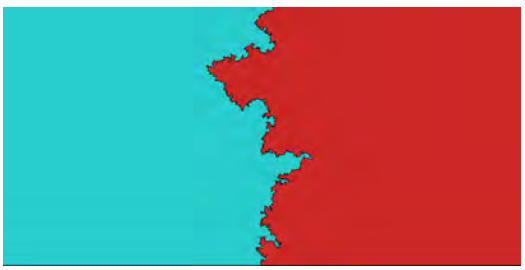
$$E[\|x_n\|^2] = n^{4/3+o(1)}$$

(pour la marche simple, le théorème central limite donne un exposant 1 au lieu de 4/3). Ces valeurs 4/3, 11/32 … portent le nom d'*exposants critiques*, et on pense qu'ils sont universels : sur un autre réseau de dimension 2, μ sera différent mais les exposants seraient les mêmes.

Plus généralement, on s'attend à ce qu'une telle grande marche ait une *limite d'échelle*, c'est-à-dire que renormalisée par son diamètre, elle converge en loi (dans la limite $n \to \infty$) vers une certaine courbe aléatoire dans le plan, comme la marche simple converge vers le mouvement brownien.

La question de la convergence reste entièrement ouverte, mais on sait quelle est cette courbe limite si elle existe : il s'agit d'une variante du processus appelé « SLE », un objet introduit par Oded Schramm en 2000 et dont l'étude a fondamentalement changé la compréhension que les mathématiciens ont de la mécanique statistique. Les travaux correspondants ont depuis été récompensés par deux médailles Fields (W. Werner en 2006 et S. Smirnov en 2010).

FIGURE 2 – Un SLE(8/3) dans le demi-plan.



1. Invariance conforme

Le cas de la marche aléatoire simple sur $\mathbb{Z}^2$ est instructif : sa limite d'échelle est explicite, il s'agit du mouvement brownien plan, qui a l'avantage de se prêter facilement à des calculs. Il a la propriété remarquable suivante : si U_1 et U_2 sont deux do-

maines simplement connexes du plan (vu comme le plan complexe) contenant 0, et si $\Phi : U_1 \xrightarrow{\sim} U_2$ est une bijection conforme envoyant 0 sur lui-même, alors pour un mouvement brownien (B_t) arrêté à sa sortie de U_1, le processus $(\Phi(B_t))$ est lui-même un mouvement brownien, arrêté à sa sortie de U_2 (à un changement de temps près).

Ce phénomène, observé pour la première fois par Lévy [7], porte le nom d'*invariance conforme*, et les physiciens prédisent qu'il devrait apparaître dans de nombreux modèles de mécanique statistique. Ils l'expliquent par la méthode du *groupe de renormalisation*, qui permet de comprendre (de manière le plus souvent non rigoureuse) l'apparition de telles symétries supplémentaires à la limite d'échelle, mais les mathématiciens sont loin de pouvoir en faire une étude (mathématiquement) rigoureuse.

Pour formaliser cette intuition dans le cadre qui va nous intéresser, la topologie la plus agréable est la suivante : pour chaque domaine simplement connexe U du plan complexe, muni de deux points marqués $a, b \in \partial U$, on cherche à définir une mesure de probabilité $\mu_{U,a,b}$ sur l'ensemble des courbes simples dans $\overline{U}$ partant de a et arrivant à b sans toucher ∂U entre-temps. Il est alors naturel d'introduire la définition suivante : une collection $(\mu_{U,a,b})$ de mesures de probabilité a la propriété d'invariance conforme si pour toute bijection conforme $\Phi : U_1 \xrightarrow{\sim} U_2$ on a l'identité $\mu_{U_2,\Phi(a),\Phi(b)} = \Phi_* \mu_{U_1,a,b}$ (autrement dit, si γ est une courbe dans U_1 de loi $\mu_{U_1,a,b}$ alors son image $\Phi(\gamma)$ a pour loi $\mu_{U_2,\Phi(a),\Phi(b)}$).

Une remarque s'impose, qui nous servira par la suite : le cas où $U_1 = U_2$ avec les mêmes points marqués est déjà non trivial, parce que Φ n'est pas pour autant l'identité, il y a une famille à un paramètre d'applications conformes qui conviennent et $\mu_{U_1,a,b}$ doit être invariante par tous les éléments de cette famille. Si par exemple U_1 est la bande $\mathbb{B} = \mathbb{R} \times (0,1)$ avec les deux points marqués à l'infini des deux côtés, on voit que $\mu_{\mathbb{B},-\infty,+\infty}$ doit être invariante par translation le long de $\mathbb{B}$. Dans le demi-plan supérieur $\mathbb{H}$ avec comme points marqués 0 et ∞, $\mu_{\mathbb{H},0,\infty}$ doit de même être invariante par changement d'échelle $z \mapsto \lambda z$ pour tout $\lambda > 0$.

2. Propriété de Markov de domaine

Une propriété qui est évidente pour la marche auto-évitante uniforme est la suivante : la loi conditionnelle des $n-k$ derniers pas, conditionnellement aux k premiers, est uniforme parmi les continuations possibles de ces k pas. Le même phénomène se produit par exemple dans le cas d'interfaces pour des modèles de mécanique statistique n'ayant que des interactions entre plus proches voisins (comme typiquement le modèle d'Ising).

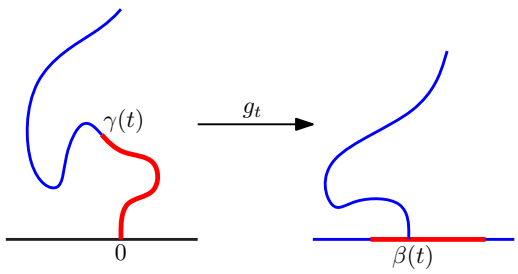
Dans le cas qui nous intéresse, on voudrait formaliser l'intuition suivante : dans un domaine U, le futur de γ sachant que son segment initial suit une portion de courbe δ a la même loi qu'une courbe dans le domaine $U \setminus \delta$, et partant de l'extrémité de δ. En notant δ^* cette extrémité et $\mu^{\delta}_{U,a,b}$ la mesure conditionnée, on dira donc que la collection $(\mu_{U,a,b})$ a la *propriété de Markov de domaine* si pour tous U, a, b, δ comme ci-dessus on a $\mu^{\delta}_{U,a,b} = \mu_{U\setminus\delta,\delta_*,b}$.

3. Chaînes de Loewner

L'observation fondamentale de Schramm [10] est alors la suivante : il n'existe qu'une famille à un paramètre de collections $(\mu_{U,a,b})$ satisfaisant à la fois à l'invariance conforme et à la propriété de Markov de domaine, et on peut les décrire explicitement.

Une façon de le voir est tout d'abord de se ramener (par invariance conforme) au cas où (U, a, b) est le demi-plan supérieur $\mathbb{H}$ avec comme points marqués 0 et ∞, puis de remarquer que la loi $\mu_{\mathbb{H},0,\infty}$ est alors entièrement déterminée par le comportement *au voisinage de* 0 de la courbe. En effet il suffit de réaliser un segment initial δ selon cette loi, et la loi de la suite de la courbe est alors obtenue comme image de $\mu_{\mathbb{H},0,\infty}$ par une application conforme de $\mathbb{H}$ vers $\mathbb{H} \setminus \delta$, qui existe par le théorème de Riemann (autrement dit, on peut « couper γ en tranches » et sa loi est caractérisée par celle de la première tranche).

FIGURE 3 – Uniformisation du complémentaire d'une courbe : l'application conforme g_t envoie $\mathbb{H} \setminus \gamma([0,t])$ sur $\mathbb{H}$.



On peut aller plus loin en suivant une stratégie introduite par Loewner [8] dans un contexte entièrement différent (il cherchait à prouver la conjecture de Bieberbach). Soit donc γ une courbe simple

dans $\mathbb{H}$, partant de 0 ; pour tout $t \geqslant 0$, notons $H_t = \mathbb{H} \setminus \gamma([0,t])$ le domaine laissé libre par γ au temps t, et soit $g_t : H_t \xrightarrow{\sim} \mathbb{H}$ l'unique application conforme telle que $g_t(z) = z + \mathcal{O}(1/z)$ à l'infini. Quitte à effectuer sur γ un changement de temps croissant, on peut même supposer que pour tout $t \geqslant 0$, le développement asymptotique de g_t est

$$g_t(z) = z + \frac{2t}{z} + \mathcal{O}(1/z^2).$$

Le théorème de Loewner énonce alors qu'il existe une fonction continue $\beta : \mathbb{R}_+ \to \mathbb{R}$ telle que (g_t) soit le flot de l'équation différentielle

$$\partial_t g_t(z) = \frac{2}{g_t(z) - \beta(t)}$$

dite *équation de Loewner*. La fonction β peut être identifiée à partir de la courbe en remarquant que

$$\beta(t) = g_t(\gamma(t)).$$

4. Le processus SLE

En combinant la construction de Loewner et l'observation de Schramm, l'identification de $(\mu_{U,a,b})$ revient à celle de $\mu_{\mathbb{H},0,\infty}$, et enfin à celle de la fonction β correspondante (qui est elle-même aléatoire). L'invariance conforme et la propriété de Markov de domaine se transposent en des propriétés de β : elle doit avoir des accroissements indépendants et stationnaires (ce qui signifie que la loi de $\beta(t+s) - \beta(t)$ ne dépend pas de t), et l'invariance de $\mu_{\mathbb{H},0,\infty}$ par changement d'échelle implique qu'en distribution,

$$\beta(\lambda t) \overset{(d)}{=} \lambda^2 \beta(t)$$

pour tous $\lambda > 0$ et $t \geqslant 0$.

Il est bien connu qu'un processus stochastique satisfaisant à ces conditions doit être un mouvement brownien, à renormalisation près : il existe un paramètre $\kappa \geqslant 0$ tel que

$$(\beta(t))_{t\geqslant 0} \overset{(d)}{=} (\sqrt{\kappa} W_t)_{t\geqslant 0}$$

où W désigne un mouvement brownien réel standard. On arrive donc à la définition :

Définition. On appelle processus (ou évolution) de Schramm-Loewner de paramètre κ, ou SLE(κ), la solution de l'équation de Loewner où l'on a posé $\beta(t) = \sqrt{\kappa} W_t$.

Une fois la définition posée, SLE(κ) désigne à la fois la famille (g_t) d'applications conformes obtenues en résolvant l'équation de Loewner, celle (H_t) de leurs domaines de définition, et la courbe γ elle-même (qui existe, mais dont l'existence ne va pas de soi à partir de la définition, la preuve [9] est extrêmement technique). On peut bien sûr étendre la définition à tout domaine simplement connexe par invariance conforme.

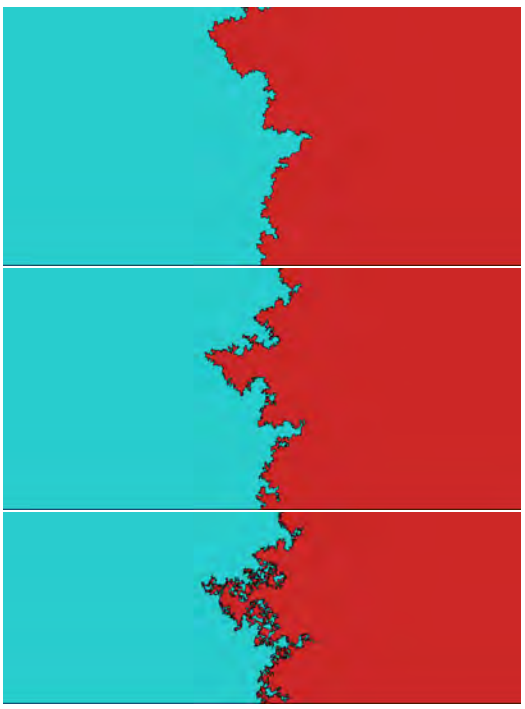
5. Propriétés du SLE

La géométrie de la courbe γ dépend fortement de la valeur du paramètre κ, ce qui est une bonne chose, car différents modèles discrets convergent vers des SLE et il serait surprenant qu'ils aient la même limite d'échelle. Par exemple, il n'est pas difficile de prouver, une fois que l'on sait que la courbe γ existe, que (avec probabilité 1 pour ces énoncés et les suivants) :

- si $\kappa \in (0,4]$, γ est une courbe simple ;
- si $\kappa \in (4,8)$, γ n'est pas une courbe simple, mais elle ne se traverse pas (elle « rebondit sur son passé ») ;
- si $\kappa \in [8,+\infty)$, γ est surjective de $\mathbb{R}_+$ vers $\overline{\mathbb{H}}$ (c'est une courbe de Peano aléatoire).

Par ailleurs, on sait [1] que sa dimension fractale est égale à $1 + \kappa/8$ pour tout $\kappa \leqslant 8$.

FIGURE 4 – Un SLE(2), un SLE(4) et un SLE(6), avec le même mouvement brownien (W_t) que dans la figure 2.



Il est également possible de calculer explicitement la probabilité de différents événements

(comme par exemple celle de toucher un intervalle prescrit de la droite réelle, ou celle de passer à droite d'un point de $\mathbb{H}$) ; le fait que tout le processus soit décrit à partir d'un mouvement brownien réel donne accès à tout l'arsenal du calcul stochastique.

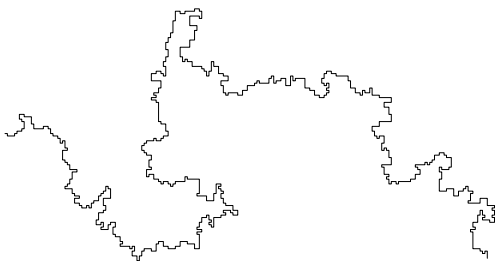
Cela donne une stratégie possible pour finir l'identification de la limite d'échelle d'un processus discret : si l'on sait obtenir l'invariance conforme et la propriété de Markov de domaine (qui est en général facile à prouver), tout ce qui reste à déterminer est la valeur du paramètre κ et cela peut être fait si l'on sait calculer, pour le modèle discret en question, la limite de la probabilité d'événements du même genre. Hélas, l'invariance conforme n'est pour l'instant connue que dans très peu de cas…

En contrepartie, tout ce que l'on sait prouver sur le SLE se transcrit en retour sur le processus discret et permet souvent d'obtenir des résultats dont l'énoncé est entièrement élémentaire, mais qui sans une telle technologie resteraient inaccessibles.

6. Exemples d'applications

Le premier cas où l'on a montré la convergence d'un modèle discret vers un SLE est celui de la *marche aléatoire à boucles effacées*, qui est (comme son nom l'indique) définie à partir de la marche aléatoire simple en supprimant de sa trajectoire toutes les boucles qu'elle forme, de manière chronologique, et ceci jusqu'à ce que la marche sorte d'un domaine discret. Il s'agit d'une marche auto-évitante aléatoire, mais dont la loi n'est *pas* uniforme, ce n'est donc pas l'objet dont nous sommes partis au début de cette note ; mais comme la marche aléatoire converge vers le brownien et que la procédure suivie est purement topologique, il est naturel de s'attendre à ce que la marche à boucles effacées ait pour limite d'échelle le « mouvement brownien à boucles effacées. »

Figure 5 – Une marche aléatoire à boucles effacées.

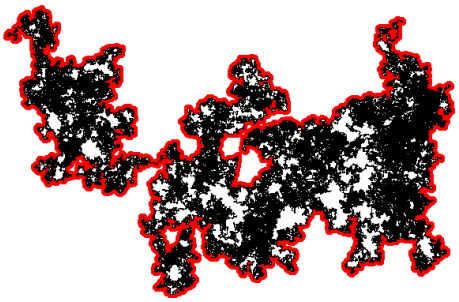


La situation n'est pas si simple (parce que le mouvement brownien fait beaucoup trop de boucles à toutes les échelles), mais il reste que l'invariance conforme est vérifiée [3] et que dans ce cas on sait prouver la convergence vers SLE pour le paramètre $\kappa = 2$. Pour revenir au modèle discret, cela permet de comprendre pourquoi après n pas, une marche à boucles effacées se trouve à une distance de l'ordre de $n^{4/5}$ de son point de départ.

D'autres modèles de mécanique statistique, par exemple la percolation [12], le modèle d'Ising [11] et les arbres couvrants uniformes [3], ont aussi des SLE pour limites d'échelle, avec à chaque fois une valeur de κ différente.

Le mouvement brownien plan lui-même est très lié au processus SLE(6) ; en particulier, ils ont des frontières extérieures de lois localement absolument continues l'une par rapport à l'autre. L'étude du SLE permet alors de prouver une conjecture due à Mandelbrot : la frontière extérieure du mouvement brownien a pour dimension 4/3 (cf. [4]).

Figure 6 – Un mouvement brownien plan (en noir) et sa frontière extérieure (en rouge).



Un dernier exemple, dont l'énoncé est entièrement élémentaire : soient (X_n) et (Y_n) deux marches aléatoires simples sur $\mathbb{Z}^2$, issues de 0, et soit, pour $N > 0$, p_N la probabilité que les trajectoires $\{X_n : 1 < n \leqslant N\}$ et $\{Y_n : 1 < n \leqslant N\}$ soient disjointes. Alors [5, 6],

$$p_N = N^{-\frac{5}{8}+o(1)}.$$

La preuve de ce fait passe par le mouvement brownien plan et le SLE(6), mais on ne sait même pas prouver l'existence de l'exposant en n'utilisant que la marche aléatoire !

7. Retour à la marche auto-évitante

Pour en revenir au problème initial : pour la marche auto-évitante uniforme, la propriété de Markov de domaine est naturelle, mais l'invariance conforme est hors de portée ; toutefois, si on la suppose vraie, on sait prouver que la limite d'échelle est un SLE(8/3) et cela permet alors de démontrer toutes les conjectures listées plus haut et de déterminer les exposants critiques. La preuve de l'invariance conforme elle-même toutefois reste inconnue ...

8. Pour en savoir plus

Le livre de Lawler [2] est une bonne introduction au SLE, et contient tous les prérequis nécessaires, à la fois en analyse complexe (pour les probabilistes) et en calcul stochastique (pour les analystes).

Références

[1] V. Beffara. « The dimension of the SLE curves ». *Ann. Probab.* **36**, n° 4 (2008), p. 1421–1452.

[2] G. F. Lawler. *Conformally Invariant Processes in the Plane*. **114**. Mathematical Surveys and Monographs. American Mathematical Society, 2005.

[3] G. F. Lawler, O. Schramm et W. Werner. « Conformal Invariance of Planar Loop-erased Random Walks and Uniform Spanning Trees ». *Ann. Probab.* **32**, n° 1B (2004), p. 939–995.

[4] G. F. Lawler, O. Schramm et W. Werner. « The Dimension of the Brownian Frontier is 4/3 ». *Math. Res. Lett.* **8** (2001), p. 13–24.

[5] G. F. Lawler, O. Schramm et W. Werner. « Values of Brownian Intersection exponents I : Half-plane Exponents ». *Acta Mathematica* **187** (2001), p. 237–273.

[6] G. F. Lawler, O. Schramm et W. Werner. « Values of Brownian Intersection exponents II : Plane Exponents ». *Acta Mathematica* **187** (2001), p. 275–308.

[7] P. Lévy. *Processus Stochastiques et Mouvement Brownien*. 2e éd. Paris : Gauthier-Villars, 1965.

[8] K. Löwner. « Untersuchungen über schlichte konforme Abbildungen des Einheitskreises. I ». *Math. Ann.* **89**, n° 1–2 (1923), p. 103–121.

[9] S. Rohde et O. Schramm. « Basic properties of SLE ». *Ann. Math.* **161**, n° 2 (2005), p. 883–924. ISSN : 0003-486X.

[10] O. Schramm. « Scaling Limits of Loop-Erased Random Walks and Uniform Spanning Trees ». *Israel Journal of Mathematics* **118** (2000), p. 221–288.

[11] S. Smirnov. « Conformal invariance in random cluster models. I. Holomorphic fermions in the Ising model ». *Ann. Math.* **172**, n° 2 (2010), p. 1435–1467.

[12] S. Smirnov. « Critical Percolation in the Plane : Conformal Invariance, Cardy's Formula, Scaling Limits ». *C. R. Acad. Sci. Paris Sér. I Math.* **333**, n° 3 (2001), p. 239–244.

Vincent Beffara

UMPA, ÉNS-Lyon, France et HCM, Bonn, Allemagne

vbeffara@ens-lyon.fr

http://perso.ens-lyon.fr/vincent.beffara/

Vincent Beffara est directeur de recherche à l'UMPA, ÉNS de Lyon, et est spécialiste en physique statistique et probabilités.

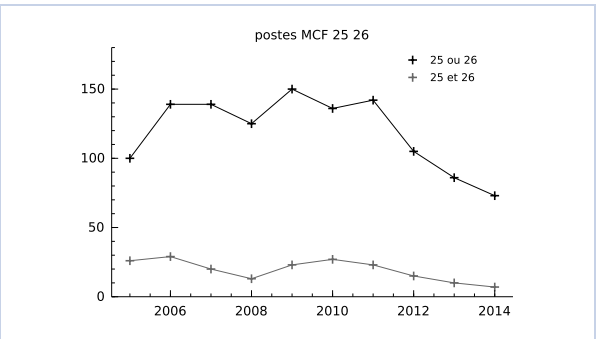
Quelques chiffres sur l'emploi en mathématique dans le domaine académique

• Y. COUDÈNE

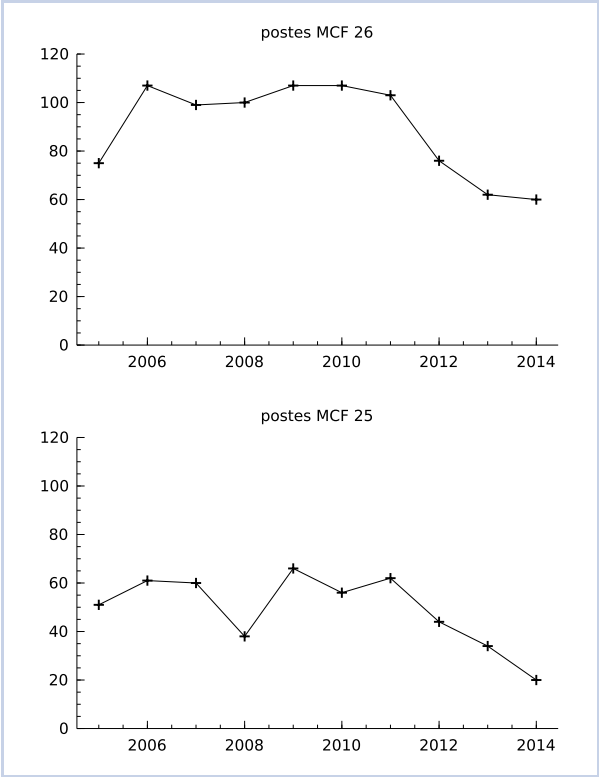
Lors d'un séminaire auquel j'ai assisté récemment, j'ai eu l'occasion d'aborder avec quelques collègues la question des postes en section 25 et 26 et des tendances générales concernant l'emploi dans le domaine des mathématiques. Il est apparu que certains collègues n'avaient pas pris l'exacte mesure des évolutions récentes, aussi ai-je compilé quelques données et réalisé des graphiques, partant du principe qu'un dessin vaut mieux qu'un long discours. Il m'a été suggéré de leur donner une diffusion plus large, les voici.

Les diagrammes suivants couvrent les dix dernières années, de 2005 à 2014 et proviennent des informations collectées sur le site de l'opération postes [1], hébergé par la SMAI. Ce site recense chaque année les offres en provenance des universités, concernant les concours maîtres de conférences et professeurs, pour les sections 25 (mathématiques), 26 (mathématiques appliquées et applications des mathématiques) et 27 (informatique). Très peu d'écoles d'ingénieurs publient leurs emplois sur le site. On peut donc considérer que ces données reflètent avant tout la situation de l'emploi en mathématique dans le domaine académique. Je me suis restreint aux profils de postes mentionnant la section 25 ou la section 26.

1. Maîtres de conférences



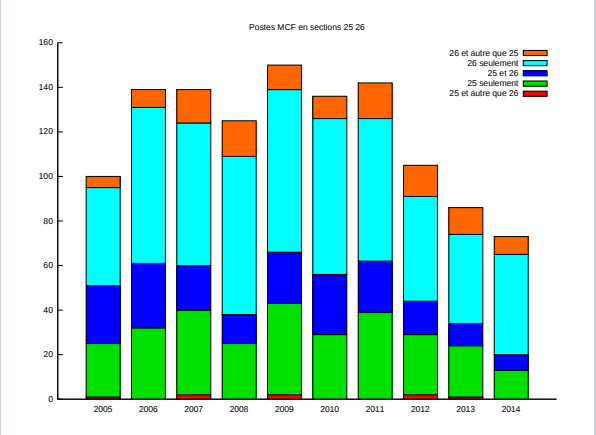
Comment lire ce diagramme : en 2009, 150 postes de maîtres de conférences mentionnaient dans leurs profils la section 25 ou la section 26. En 2014, ils n'étaient plus que 73. En 2014, 7 postes mentionnaient à la fois les sections 25 et 26 dans leurs profils, contre 23 en 2009.



Comment lire ces diagrammes : en 2009, 66 postes de maîtres de conférences mentionnaient dans leurs profils la section 25. En 2014, ils n'étaient plus que 20. En 2014, 60 postes mentionnaient la section 26 dans leurs profils, contre 107 en 2009.

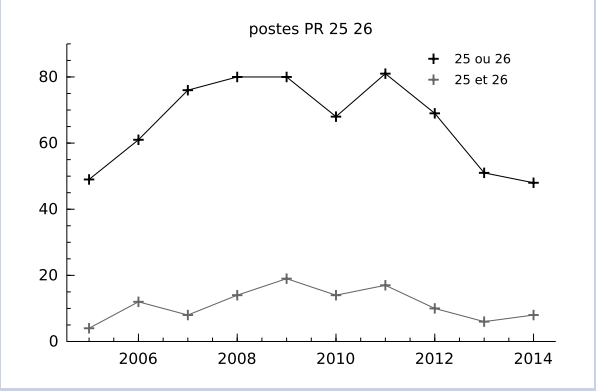
1. http://postes.smai.emath.fr

Le graphique suivant reprend les informations précédentes, tout en précisant la répartition des postes par section, année après année.

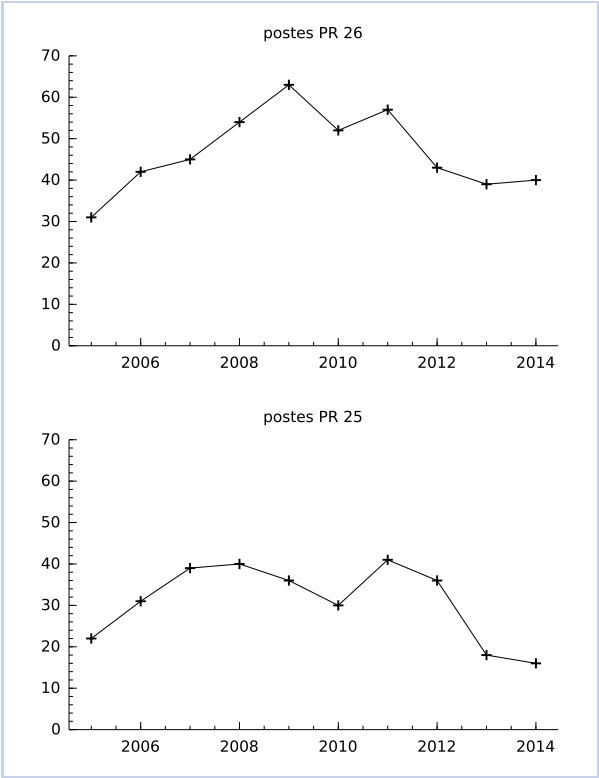


Comment lire ce diagramme : sur les 150 postes mis au concours en 2009 en section 25 ou 26, 2 sont fléchés en section 25 ainsi que dans une ou plusieurs autres sections toutes différentes de 26, 41 postes ont la section 25 comme unique profil, 23 ont un profil contenant la section 25 et la section 26, 73 ont la section 26 comme unique profil et 11 sont fléchés en section 26 ainsi que dans une ou plusieurs autres sections toutes différentes de 25.

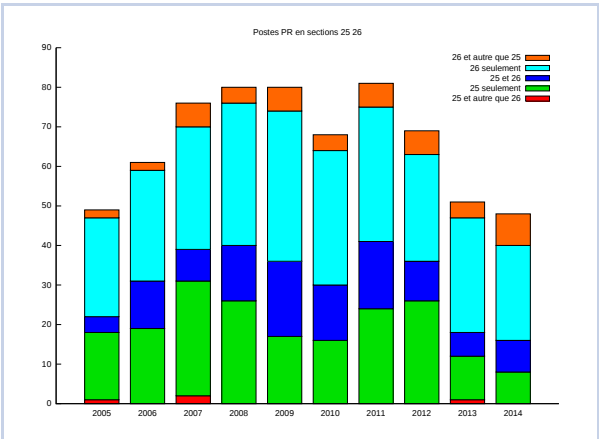
2. Emplois de professeurs d'université



Comment lire ce diagramme : en 2009, 80 postes de professeurs mentionnaient dans leurs profils la section 25 ou la section 26. En 2014, ils n'étaient plus que 48. En 2014, 8 postes mentionnaient à la fois les sections 25 et 26 dans leurs profils, contre 19 en 2009.



Comment lire ces diagrammes : en 2009, 36 postes de professeurs mentionnaient dans leurs profils la section 25. En 2014, ils n'étaient plus que 16. En 2014, 40 postes mentionnaient la section 26 dans leurs profils, contre 63 en 2009.



Comment lire ce diagramme : sur les postes mis au concours en 2009 en section 25 ou 26, 17 postes ont la section 25 comme unique profil, 19 ont un profil contenant la section 25 et la section 26, 38 ont la section 26 comme unique profil et 6 sont fléchés en section 26 ainsi que dans une ou plusieurs autres sections toutes différentes de 25.

En résumé, le nombre de postes entre 2009 et 2014 a été divisé par 3 en section 25 et par 2 en section 26. Toutes mes félicitations à ceux et celles qui viennent d'être recrutés en 2014. Une motion des sections 25 et 26 du CNU (février 2014) alerte les pouvoirs publics sur la situation actuelle et propose quelques solutions. `http://cnu25.emath.fr/motions/Motion12-030214.pdf`

Yves Coudène

Université de Bretagne Occidentale, 6 avenue Le Gorgeu, 29238 Brest cedex 3, France

`yves.coudene@univ-brest.fr`

Yves Coudène est professeur des universités. Ses travaux se situent dans le domaine des systèmes dynamiques, de la théorie ergodique et de la géométrie en courbure négative.

Prix Fermat 2015

La nouvelle édition du Prix Fermat en recherche mathématique est lancée en mars 2015, l'appel aux candidatures et à leurs parrainages sera ouvert jusqu'au 30 juin 2015 et la proclamation du résultat aura lieu en décembre 2015.

Le Prix Fermat récompense les travaux de recherche d'un ou de plusieurs mathématiciens dans des domaines où les contributions de Pierre de Fermat ont été déterminantes :

- énoncés de principes variationnels, ou plus généralement équations aux dérivées partielles,
- fondements du calcul des probabilités et de la géométrie analytique,
- théorie des nombres.

À l'intérieur de ces domaines, l'esprit du prix est de récompenser plutôt des résultats de recherche qui sont accessibles au plus grand nombre de mathématiciens professionnels.

Plus de détails notamment sur la procédure de candidature sont disponibles :

`http://www.math.univ-toulouse.fr/PrixFermat`

`http://www.math.univ-toulouse.fr/FermatPrize`

Journée annuelle de la SMF

Les mathématiques sont partout, y compris dans les entreprises, petites ou grandes. Cette affirmation banale mérite réflexion. Le 26 juin prochain à l'IHP se tiendra la journée annuelle 2015 de la SMF ; ce sera l'occasion d'entendre des témoignages, d'échanger sur les données chiffrées et de voir des mathématiques s'inviter de façon inattendue dans des histoires d'entreprises.

Une enquête récente commanditée par AMIES cherche à évaluer le rôle des mathématiques dans la prospérité du pays. Les résultats méritent d'être expliqués, illustrés et débattus, avec en filigrane la question suivante « Comment utiliser ces données pour consolider le financement des mathématiques et faciliter l'insertion de jeunes mathématiciens dans les entreprises ? »

Le programme est disponible à l'adresse :

`smf.emath.fr/journée-annuelle-2015-paris`

BIG SISTER GAZETTE

La Gazette est à la pointe des techniques modernes. Il convient, de plus en plus, d'utiliser les ressources disponibles afin de réduire d'autant le travail du secrétariat de rédaction.

1. La Gazette est composée à l'Institut Fourier à Grenoble en TEX, sur un ordinateur SM90. Les textes composés en TEX peuvent donc être envoyés par la poste sur disquette 5 1/4. Inutile dans ce cas d'y inclure vos normes de composition, la Gazette a les siennes. Joignez y toujours en revanche une sortie papier.

2. On peut aussi envoyer les fichiers TEX par Bitnet aux adresses suivantes :
monika at frcicg71
andler at frulm63.

3. On peut aussi envoyer (par la poste) des disquettes Macintosh à Martin Andler, qui les transformera, en utilisant le prototype Easytex, en fichiers TEX, puis les transmettra à Grenoble.

4. On peut joindre le Comité de rédaction par Minitel sur la messagerie du CNRS (MICNRS sur le 36 13), à l'adresse AndlerM1.

5. Tout cela ne veut pas dire que le Comité de rédaction renonce, de quelque façon que ce soit, à son contrôle sur le contenu de la Gazette. Tous les textes doivent lui être soumis avant publication.

6. La Gazette a besoin des mathématiciens pour des articles de toutes natures. N'hésitez pas à nous contacter pour nous faire part de vos propositions, souhaits et projets.

Louis Boutet de Monvel
1941-2014

• B. Helffer

Louis Boutet de Monvel est décédé le jour de Noël des suites d'une longue maladie. Le 6 janvier, une salle trop petite au cimetière du Père Lachaise a rassemblé sa famille, ses collègues et amis pour un dernier adieu. Claude Bardos, Jean-Michel Bony, François Golse, Joseph Oesterlé et la sœur de Louis ont évoqué avec émotion, humour et tendresse sa carrière, son dévouement, son œuvre, sa manière de chercher et tout ce qu'il était aussi en dehors des mathématiques.

1. Sa carrière

Dans le texte qui suit j'évoquerai quelques aspects de sa carrière et de son œuvre. Une analyse plus détaillée des travaux de ce grand mathématicien est bien sûr impossible dans un texte aussi court. Louis est né le 22-6-1941 à Issy-les-Moulineaux. Après des études primaires et secondaires au Lycée français de Londres jusqu'en 1955, il poursuit au Lycée Louis-le-Grand de 1956 à 1960. Il rentre à l'ÉNS en 1960. Louis a enseigné à Alger (67-69), puis il a été professeur aux universités de Nice (69-71), de Paris 7 (71-75), de Grenoble (75-79) avant de prendre un poste à l'université Paris VI et de diriger le centre de mathématiques de l'ÉNS (de 1978 à 1985).

Comme l'a évoqué J.-M. Bony, on peut trouver l'origine de son orientation scientifique dans sa participation active au fameux séminaire Cartan-Schwartz de 63-64 sur la formule de l'indice d'Atiyah-Singer. La liste des intervenants est éloquente : Cartan et Schwartz bien sûr mais aussi les jeunes Morlet, Illusie, Krée, Baouendi, J. Bokobza, Grisvard, A. Unterberger, pour ne citer que les participants à la première partie. Louis y fait deux exposés sur la transformation des opérateurs de Caledròn Zygmund par difféomorphisme et sur le passage de la dimension paire à la dimension quelconque. Il devient élève de Laurent Schwartz et soutient sa thèse d'état en 1969, thèse très impressionnante puisqu'elle lui valut d'être conférencier invité au Congrès International des Mathématiciens qui se déroula à Nice en 1970.

Du séjour de Louis à Grenoble, Bernard Malgrange [1] se souvient de sa participation systématique et enthousiaste au séminaire de ski de fond (en saison) et du séminaire qu'ils ont organisé avec Monique Lejeune, en 75-76 sur les opérateurs différentiels et pseudodifférentiels. Ce séminaire a servi de référence à l'époque sur ce sujet (D-modules, opérateurs pseudodifférentiels analytiques, etc.), qui en était à ses débuts.

De l'avis même de Louis son travail de directeur à l'ÉNS pendant sept années fut dans sa carrière son activité la plus prenante et la plus intéressante. C'est entre autres l'époque (79-82) où il organise le séminaire *Mathématique et Physique* avec Adrien Douady et Jean-Louis Verdier.

Il revient à plein temps à Paris 6 à partir de 1985 et devient président de la commission de spécialistes à partir de 1988. Sur son activité administrative, il écrivit un jour : « J'ai pris part normalement au travail collectif nécessaire à la bonne marche de l'Université ».

Louis fut aussi un collaborateur de Bourbaki (1971-1991). Il a dirigé de nombreuses thèses (une trentaine). Bien que mon directeur de thèse fut officiellement Charles Goulaouic, j'ai toujours indiqué qu'il était mon deuxième directeur, tant ses conseils et ses encouragements furent décisifs lors de l'achèvement de ma thèse d'état (1976), sans oublier la belle expérience de coopération avec lui

1. Communication personnelle de janvier 2015.

qui prit naissance à l'institut Mittag-Leffler durant l'hiver 1974. Il fut aussi le directeur de Gilles Lebeau [2] (1983) qu'il a toujours considéré comme son meilleur élève. Enfin on ne peut oublier sa participation au CNU (73-75, 78-95) pendant de nombreuses années où il apporta sa large compétence scientifique pour les évaluations.

Il a reçu de nombreux prix dont la médaille Émile Picard de l'Académie des Sciences (2007) et fut élu « Foreign Honorary Member » à l'American Academy of Arts and Sciences en avril 2012.

2. Sur son œuvre

Louis a beaucoup contribué au développement de l'analyse microlocale dans les années 70. Ses travaux sur les opérateurs pseudodifférentiels analytiques, le traitement pseudo-différentiel des problèmes aux bord et de l'hypoellipticité des opérateurs à caractéristiques multiples font autorité.

Il a aussi d'importantes contributions en analyse complexe (étude du noyau de Bergman avec Johannes Sjöstrand) et a beaucoup travaillé sur les opérateurs de Toeplitz (travaux avec Victor Guillemin), la théorie de l'indice et à partir des années 90 sur les star-produits.

Ses travaux (une centaine d'articles) dépassent alors largement le cadre de l'analyse des EDP et mettent en évidence sa maîtrise impressionnante de la géométrie, de la topologie algébrique et de la physique mathématique. J'ai listé dans la bibliographie ci-dessous la plupart des références que Louis avait lui-même choisies pour ses Selecta [3]. Elles ont été classées par thème (problèmes aux limites[1, 2], opérateurs pseudo-différentiels analytiques [3, 4], opérateurs pseudo-différentiels à caractéristiques doubles [5, 6], noyaux de Bergman et de Szegö [7, 8], opérateurs de Toeplitz [9, 10, 11, 12, 13], star-produits [14, 15] et divers [16, 17, 18, 19, 20, 21]) et apparaissent dans cet ordre dans la bibliographie ci-dessous. Une liste complète (à l'époque) a été publiée en 2004 aux Annales de l'Institut Fourier. Outre des publications dans des revues prestigieuses, il me semble important de remarquer que de nombreux travaux très cités ne sont parus que dans des séminaires et principalement dans le séminaire de l'École polytechnique lancé par C. Goulaouic et L. Schwartz dans les années 70 et qui sous divers noms continue de se réunir mensuellement.

Références

[1] L. Boutet de Monvel. « Comportement d'un opérateur pseudo-différentiel sur une variété à bord. I. La propriété de transmission ». *J. Analyse Math.* **17** (1966), p. 241–253. ISSN : 0021-7670.

[2] L. Boutet de Monvel. « Boundary problems for pseudo-differential operators ». *Acta mathematica* **126**, n° 1 (1971), p. 11–51.

[3] L. Boutet de Monvel et P. Krée. « Pseudodifferential operators and Gevrey classes ». *Ann. Inst. Fourier 17* (1967), p. 295–323.

[4] L. Boutet de Monvel. « Opérateurs pseudo-différentiels analytiques et problèmes aux limites elliptiques ». In : *Annales de l'institut Fourier*. Vol. 19. 2. Institut Fourier. 1969, p. 169–268.

[5] L. Boutet de Monvel. « Hypoelliptic operators with double characteristics and related pseudo-differential operators ». *Communications on Pure and Applied Mathematics* **27**, n° 5 (1974), p. 585–639.

[6] L. Boutet de Monvel, A. Grigis et B. Helffer. « Parametrixes d'opérateurs pseudo-différentiels à caractéristiques multiples ». In : *Journées : Équations aux Dérivées Partielles de Rennes (1975)*. Astérisque 34–35. Soc. Math. France, Paris, 1976, p. 93–121.

[7] L. Boutet de Monvel. « Intégration des équations de Cauchy-Riemann induites formelles ». *Séminaire Goulaouic-Schwartz, Ecole polytechnique, Exposé 9* (1975-76).

[8] L. Boutet de Monvel et J. Sjöstrand. « Sur la singularité des noyaux de Bergman et de Szegő ». In : *Journées : Équations aux Dérivées Partielles de Rennes (1975)*. Astérisque 34–35. Soc. Math. France, Paris, 1976, p. 123–164.

[9] L. Boutet de Monvel. « On the index of Toeplitz operators of several complex variables ». *Inventiones mathematicae* **50**, n° 3 (1978), p. 249–272.

[10] L. Boutet de Monvel. « Opérateurs à coefficients polynomiaux, espace de Bargmann, et opérateurs de Toeplitz ». *Séminaire Goulaouic-Meyer-Schwartz, Ecole polytechnique, Exposé 1* (1980-81).

[11] L. Boutet de Monvel et V. Guillemin. *The spectral theory of Toeplitz operators*. **99**. Annals of Mathematics Studies. Princeton University Press, Princeton, NJ; University of Tokyo Press, Tokyo, 1981, p. v+161. ISBN : 0-691-08284-7; 0-691-08279-0.

2. Voir le texte de G. Lebeau dans la lettre de l'INSMI de janvier 2015.

3. Édition en préparation chez Springer sous la responsabilité éditoriale de V. Guillemin et J. Sjöstrand avec la coopération d'Anne Boutet de Monvel.

[12] L. Boutet de Monvel. « Opérateurs pseudodifférentiels à bicaractéristiques périodiques ». *Séminaire Bony-Meyer-Schwartz, École polytechnique, Exposé 20* (1984-85).

[13] L. Boutet de Monvel. « Symplectic cones and Toeplitz operators ». In : *Multidimensional complex analysis and partial differential equations (São Carlos, 1995)*. Vol. 205. Contemp. Math. Amer. Math. Soc., Providence, RI, 1997, p. 15–24.

[14] L. Boutet de Monvel. « Star products on conic Poisson manifolds of constant rank ». *Mat. Fiz. Anal. Geom.* **2**, n° 2 (1995), p. 143–151. ISSN : 1027-1767.

[15] L. Boutet de Monvel. « Complex star algebras. » *Math. Phys. Anal. Geom.* **2**, n° 2 (1999), p. 113–139.

[16] L. Boutet de Monvel. « Convergence dans le domaine complexe des séries de fonctions propres ». *C. R. Acad. Sci. Paris Sér. A-B* **287**, n° 13 (1978), A855–A856.

[17] L. Boutet de Monvel. « D-modules holonômes réguliers en une variable ». *Mathématiques et Physique, Séminaire de L'ÉNS* **1979-1982** (1983), p. 313–321.

[18] L. Boutet de Monvel et B. Malgrange. « Le théorème de l'indice relatif ». In : *Annales scientifiques de l'École normale supérieure*. Vol. 23. 1. Société mathématique de France. 1990, p. 151–192.

[19] L. Boutet de Monvel. « Indice des systèmes différentiels ». In : *D-modules, Representation Theory, and Quantum Groups*. Springer, 1993, p. 1–30.

[20] A. Boutet de Monvel-Berthier, L. Boutet de Monvel et G. Lebeau. « Sur les valeurs propres d'un oscillateur harmonique perturbé ». *J. Anal. Math.* **58** (1992). Festschrift on the occasion of the 70th birthday of Shmuel Agmon, p. 39–60.

[21] L. Boutet de Monvel. « On the holonomic character of the elementary solution of a partial differential operator ». *New trends in Microlocal Analysis, Springer–Verlag Tokyo* (1997), p. 171–178.

Bernard Helffer

Laboratoire de mathématiques de l'université Paris Sud, 91405 Orsay cedex, France

Bernard.Helffer@math.u-psud.fr

Bernard Helffer est professeur émérite de l'université Paris-Sud et chercheur associé au Laboratoire de Mathématiques Jean Leray de l'université de Nantes. Il est spécialiste en équations aux dérivées partielles, en théorie spectrale et en physique mathématique.

Denis Feyel

1944-2015

Denis Feyel nous a quittés le mois de janvier dernier, au terme d'une longue maladie. Ancien élève de l'École normale supérieure (1963), il a commencé sa carrière comme maître-assistant à l'université Paris 6, puis a été professeur à l'université d'Évry, de 1992 à sa retraite en 2009. Il a également enseigné deux ans à Wuhan (entre 1983 et 1985), dans le cadre de la classe sino-française de mathématiques. Très engagé dans la communauté des potentialistes, Denis a été le directeur du comité éditorial de la revue *Potential Analysis* dès sa fondation en 1992. Le thème principal de ses recherches à l'université Paris 6 (où il soutint sa thèse d'État en 1979) aura été la théorie du potentiel. Puis, assez naturellement, à partir du milieu des années 80, il s'est tourné vers l'analyse en dimension infinie, principalement sur l'espace de Wiener. Les deux articles, avec A. de La Pradelle : « Espaces de Sobolev gaussiens » (*Ann. Inst. Fourier*, 1989) et « Capacités gaussiennes » (*Ann. Inst. Fourier*, 1991), ont amené un point de vue tout à fait original et particulièrement fécond dans l'analyse sur l'espace de Wiener (et plus généralement sur les espaces gaussiens) ainsi que sur le calcul différentiel stochastique (calcul de Malliavin). Il faut aussi noter la série d'articles fondamentaux écrits avec A.S. Üstünel sur la théorie du transport de mesures sur l'espace de Wiener (notamment, « Monge-Kantorovitch measure transportation and Monge-Ampère equation on Wiener space », *Probab. Th. and Rel. Fields*, 2004). Un texte d'hommage rédigé à la demande de ses collègues et anciens élèves est consultable sur le site du laboratoire d'Evry (`http://www.math-evry.cnrs.fr/pmf/denis_feyel`) et sur le site de la SMF (`http://smf.emath.fr/files/denis_feyel.pdf`).

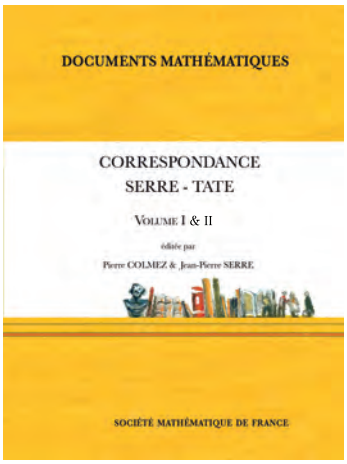
La maison des mathématiques
Cédric Villani, Jean-Philippe Uzan et Vincent Moncorgé
Le Cherche-Midi, 2014. 144 p. ISBN : 978-2749133539

L'Institut Henri Poincaré (IHP) « est un outil unique au monde pour les sciences mathématiques. Situé au cœur de Paris et entouré de nombreux établissements universitaires prestigieux, c'est un lieu de rencontres officielles et informelles pour les scientifiques, français ou non ». Ainsi commence le court texte du célèbre physicien mathématicien Joel Lebowitz, dans le tout récent livre « *La maison des mathématiques* » consacré à cet institut, et édité par le Cherche-Midi.
Ce livre, destiné au grand public, célèbre les vingt ans de la renaissance de l'institut en 1994, après une première création en 1928 et son quasi-abandon lors de la refonte des universités en 1968. C'est un ouvrage original et hétéroclite. À deux longs textes du directeur Cédric Villani et de son adjoint Jean-Philippe Uzan, sont adossés une quinzaine de textes, d'une ou deux pages, de diverses personnalités ayant participé à la vie de l'institut, ainsi que de nombreuses photographies de Vincent Moncorgé. Ce dernier a pris sur le vif les chercheurs au travail dans les couloirs, les bureaux et les amphithéâtres de l'institut.
Dans son texte, Cédric Villani présente l'histoire et l'organisation de l'IHP, tout en nous livrant de nombreuses anecdotes. On y apprend par exemple que, dans les années 1930, Albert Einstein y a enseigné la relativité générale et que Fritz London y a compris le lien entre la condensation de Bose-Einstein et la superfluidité. Malgré ces succès, la physique théorique n'a été officiellement associée aux mathématiques à l'IHP qu'en 1994. D'un autre côté, la frontière entre les deux sciences était moins claire au début du vingtième siècle, comme le rappellent les travaux de Poincaré lui-même.
Jean-Philippe Uzan disserte, lui, de questions plus philosophiques. Quel rôle jouent les mathématiques vis-à-vis des autres sciences ? Comment expliquer la « déraisonnable efficacité des mathématiques » pour décrire notre monde (remarquée par Eugene Wigner dans un célèbre article de 1960) ? Mais, d'un autre côté, comment expliquer les petits désaccords récurrents entre la théorie et l'expérience ? Sans oublier non plus la« déraisonnable inefficacité des mathématiques en biologie », relevée par Israel Gelfand. Le texte de Jean-Philippe Uzan est accessible à tous. Les mathématiques y sont présentées comme très vivantes et en interaction permanente avec les autres sciences, sans que l'auteur n'oublie bien sûr leur aspect plus artistique voire ésotérique, fréquemment mis en avant.
Les autres témoignages concernent tous les aspects de l'institut : les activités du centre Émile Borel, la bibliothèque, les sociétés savantes, les diverses autres associations hébergées à l'IHP, les éditions scientifiques, etc.
Je voudrais terminer avec quelques mots concernant les photographies de Vincent Moncorgé, qui constituent la plus grande part du livre et qui sont actuellement exposées sur les murs de l'IHP. Le photographe explique tout à la fin de l'ouvrage, avec humour, qu'il a eu carte blanche pour capter la vie de l'institut pendant près de deux ans... « sans rien comprendre de ce qu'il a pu lire ou entendre ». Son travail est une belle réussite. L'élément central de la plupart des clichés est le tableau noir, vu comme objet principal de communication entre les chercheurs. Ce choix a fourni des clichés très contrastés, où la craie blanche ressort franchement et où les chercheurs semblent parfois se fondre avec le tableau. On y voit peu d'ordinateurs, de feuilles de papier et de tasses de café. Bien sûr, on pourrait regretter l'absence de légende permettant de savoir qui est qui, mais ceci est

certainement une conséquence du fait que le photographe a arpenté les lieux« clandestinement ». Les dernières pages sont des clichés des fameux modèles mathématiques, dont certains sont visibles à la bibliothèque. Ils avaient déjà intrigué Man Ray dans les années 30, et ont représenté un tournant important dans son œuvre. L'IHP aura-t-il une telle influence sur l'œuvre de Vincent Moncorgé ?

Mathieu Lewin
Université Paris Dauphine

la Gazette des Mathématiciens



Documents Mathématiques

Correspondance Serre-Tate (volumes I & II)

Pierre Colmez et Jean-Pierre Serre, éditeurs
Société Mathématique de France, 2015. 969 pages
ISBN : 978-85629-803-4

Ces deux volumes reproduisent, avec notes et commentaires, la correspondance entre Jean-Pierre Serre et John Tate de 1956 à 2000. Ils contiennent également un choix de mels postérieurs à l'année 2000. Les textes sont reproduits dans leur langue originale : tantôt en anglais et tantôt en français. La plupart datent des vingt années 1956-1976. Ils évoquent des questions telles que la rédaction des Éléments de Bourbaki, la cohomologie galoisienne, la géométrie rigide, les conjectures de Tate sur les cycles algébriques, les groupes formels et p-divisibles, la multiplication complexe, et les formes modulaires : propriétés de congruence, formes de poids 1, représentations galoisiennes. Ces volumes devraient être utiles aux amateurs de théorie des nombres, ainsi qu'aux historiens des mathématiques.

Prix public : 140 € – Prix membre SMF : 98 € – Frais de port non compris

These two volumes reproduce, with notes and comments, the correspondence between Jean-Pierre Serre and John Tate from 1956 to 2000. They also contain a choice of e-mails post-2000. The texts are reproduced in their original language: in English or in French. Most of them are from the 20 years 1956-1976.They treat questions like the write-up of Bourbaki's Elements, Galois cohomology, rigid geometry, Tate's conjectures on algebraic cycles, formal and p-divisible groups, complex multiplication, and modular forms: congruence properties, weight 1 forms, Galois representations. These volumes should be useful to people interested in Number Theory or History of Mathematics.

Public price: 140 € – SMF member price: 98 € – Shipping costs not included

Société Mathématique de France
SMF

http://smf.emath.fr