Interview des lauréats du prix Abel 2021
László Lovász et Avi Wigderson
Bjørn Ian Dundas et Christian F. Skau

Professeur Lovász et Professeur Wigderson. Tout d'abord, nous tenons à vous féliciter d'être les lauréats du prix Abel 2021. Nous citons le comité Abel :

> *"Pour leurs contributions fondamentales à l'informatique théorique et aux mathématiques discrètes, et leur rôle de premier plan d'en avoir fait des domaines centraux des mathématiques modernes."*

Nous voudrions d'abord que vous commentiez le changement remarquable qui s'est produit au cours des dernières décennies dans l'attitude, disons, des mathématiques dominantes envers les mathématiques discrètes et l'informatique théorique. Comme vous le savez parfaitement, il n'y a pas si longtemps, il était assez courant chez de nombreux mathématiciens de première classe d'avoir une opinion sceptique, voire condescendante, pour ce type de mathématiques.

Pouvez-vous commencer, professeur Lovász, s'il vous plaît ?

Lovász : Je pense que c'est vrai. Il a fallu du temps avant que deux choses ne soient réalisées à propos de l'informatique théorique qui sont pertinentes pour les mathématiques.

L'une d'elle est simplement que l'informatique théorique est une source de problèmes passionnants. Quand j'ai terminé mes études à l'université, avec d'autres jeunes chercheurs, nous avons créé un groupe pour étudier le calcul et l'informatique, car nous avons réalisé que c'était un domaine très inexploré couvrant des questions sur ce qui peut être calculé, à quelle vitesse et avec quelle précision, etc.

La deuxième chose est que lorsque les réponses ont commencé à venir, en particulier lorsque les notions de NP et P, i.e. de temps polynomial non-déterministe et de temps polynomial sont devenues centrales, nous nous sommes rendu compte que l'ensemble des mathématiques pouvait être vu d'une manière complètement différente à travers ces notions, par le calcul efficace et par les courtes preuves d'existence.

Pour nous jeunes gens, ces deux choses étaient si inspirantes que nous avons commencé à établir des liens avec le reste des mathématiques. Je pense qu'il a fallu du temps jusqu'à ce que des personnes d'autres domaines des mathématiques réalisent la portée de cela, mais peu à peu ça s'est fait. En théorie des nombres, cela s'est avéré très important, et aussi en théorie des groupes, ces notions

Bjørn I.Dundas : Université de Bergen, Christian F. Skau : Université norvégienne de Science et technologie, Trondheim, Norvège.
Article mis librement en ligne par la Société européenne des mathématiques (European Mathematical Society, EMS) ici https://ems.press/journals/mag/articles/3718591.
Référence : Bjørn Ian Dundas, Christian F. Skau, Abel interview 2021: László Lovász and Avi Wigderson, Eur. Math. Soc. Mag. 122 (2021), pp. 16-31, DOI 10.4171/MAG-54

Transcription et correction de la traduction fournie par les outils Google traduction, Denise Vella-Chemla, février 2022.

sont devenues importantes, puis lentement dans de nombreux autres domaines des mathématiques.

WIGDERSON : Oui, je suis complètement d'accord. En fait, il est vrai qu'il y avait une attitude condescendante chez certains mathématiciens envers les mathématiques discrètes. Ça l'était peut-être moins pour l'informatique théorique, parce qu'elle existait dans le domaine de l'informatique au fur et à mesure qu'elle se développait, et peut-être que les gens en étaient moins conscients directement ? Je pense que Lovász a raison dans la mesure où l'idée même d'algorithmes efficaces et les notions de complexité computationnelle qui ont été introduites en informatique théorique sont fondamentales pour les mathématiques, et il a fallu du temps pour s'en rendre compte.

Cependant, la vraie vérité est que tous les mathématiciens de tous âges ont tous utilisé des algorithmes. Ils avaient besoin de calculer des choses. Le célèbre défi de Gauss à la communauté mathématique de trouver des méthodes rapides pour tester si un nombre est premier et pour factoriser des nombres entiers est extrêmement éloquent, compte tenu de l'époque à laquelle il a été écrit. Cela demande vraiment que des algorithmes rapides soient développés.

Certaines parties des mathématiques discrètes étaient considérées par certains comme triviales dans le sens où il n'y a qu'un nombre fini de possibilités que nous devons tester. Alors, en principe, cela peut être fait, donc quel est le problème ?

Je pense que la notion d'algorithme efficace clarifie le problème. Il peut y avoir un nombre exponentiel de choses à essayer, et vous ne le ferez jamais, n'est-ce pas ? Si à la place vous avez un algorithme rapide pour le faire, alors cela fait toute la différence. La question de savoir si un tel algorithme existe devient primordiale.

Cette compréhension a évolué. Elle a d'abord attrapé les pionniers des années 70 dans le domaine de la combinatoire et dans le domaine des mathématiques discrètes, parce que là, c'est plus naturel ; au moins, il est facile de formuler des problèmes, de sorte que vous pouvez leur attacher une certaine complexité. Peu à peu, la compréhension s'est étendue à d'autres parties des mathématiques. La théorie des nombres en est un excellent exemple, car là aussi, il existe des problèmes discrets et des méthodes discrètes qui se cachent derrière de nombreux résultats théoriques célèbres. De là, cette compréhension s'est peu à peu disséminée. Je pense qu'elle est maintenant suffisamment universelle pour que soit comprise l'importance des mathématiques discrètes et de l'informatique théorique.

Turing et Hilbert

C'est certes une question naïve, mais en tant que non-experts, nous avons peu d'inhibitions, alors voici : pourquoi la notion de Turing de ce qu'on appelle aujourd'hui une machine de Turing capture-t-elle l'idée intuitive d'une procédure efficace, et, pour ainsi dire, établit la norme pour ce qui peut être calculé ? Quel est le lien avec le problème dit Entscheidungsproblem de Hilbert ?

WIGDERSON : Je pense que ma première recommandation serait de lire l'article de Turing - en fait, de lire *tous* ses articles. Il écrit avec tant d'éloquence. Si vous lisez son article sur les procédures informatiques et le problème dit Entscheidungsproblem, vous comprendrez tout.

Il y a plusieurs raisons pour lesquelles la machine de Turing est si fondamentale et si basique. La première est qu'elle est simple - elle est extrêmement simple. C'était évident pour Turing et pour beaucoup d'autres à cette époque. C'est si simple que ça pourrait être implémenté directement. Et c'est ainsi qu'il a lancé la révolution informatique. Si vous regardez d'autres notions de calculabilité que les gens ont étudiées, Gödel et d'autres - certainement Hilbert - avec des fonctions récursives et ainsi de suite, elles ne se prêtaient pas à la fabrication d'une machine en sortie. Donc c'était fondamental.

La seconde est que quelques années plus tard il a été prouvé que toutes les autres notions de calculabilité efficace étaient équivalentes. La machine de Turing pourrait donc toutes les simuler. Elle les englobait toutes, mais elle était beaucoup plus simple à décrire.

Troisièmement, une façon pour Turing de motiver son modèle est de regarder ce que nous, les humains, faisons lorsque nous calculons pour résoudre un problème, disons multiplier deux nombres longs. Regardez ce que nous faisons sur une feuille de papier, nous rendons le problème abstrait et le formalisons. Et quand nous faisons cela, nous sommes automatiquement amenés à un modèle tel que la machine de Turing.

La quatrième raison est l'universalité, le fait que son modèle est un modèle universel. Dans une seule machine, vous pouvez avoir une partie des données qui est un programme que vous souhaitez exécuter, et cela émulera simplement ce programme. C'est pourquoi nous avons des ordinateurs portables, des ordinateurs, etc. Il n'y a qu'une seule machine. Vous n'avez pas besoin d'avoir une machine pour multiplier, une machine différente pour intégrer, une machine encore différente pour tester la primalité, etc. Vous n'avez qu'une seule machine dans laquelle vous pouvez écrire un programme. C'était une révolution incroyable et elle encapsule cela dans une notion vraiment simple que tout le monde peut comprendre et utiliser, donc cette notion est puissante.

Maintenant, vous avez posé une question sur la relation avec le problème appelé Entscheidungsproblem. Vous savez, Hilbert avait un rêve, et le rêve avait deux parties : tout ce qui est vrai en mathématiques est prouvable, et tout ce qui est prouvable peut être calculé automatiquement. Eh bien, Gödel a brisé le premier rêve - il y a des faits vrais, disons, sur les nombres entiers, qui ne peuvent pas être prouvés. Et puis Church et Turing ont brisé le second rêve. Ils ont montré qu'il y a des choses prouvables qui ne sont pas calculables. La preuve de Turing est non seulement beaucoup plus simple que celle de Gödel, avec l'argument diagonal rusé de Turing, elle implique également le résultat de Gödel si vous y réfléchissez. C'est généralement ainsi que la plupart des gens enseignent la théorie de l'incomplétude de Gödel aujourd'hui ; eh bien, je ne sais pas si "la plupart des gens" seraient d'accord avec ça, mais cela utilise les notions de Turing. C'est donc ç, la connexion. Turing s'est bien sûr inspiré des travaux de Gödel. Tout ce qui l'a amené à travailler sur la calculabilité, ça a été le travail de Gödel.

LOVÁSZ : J'ai juste une chose que je voudrais ajouter. Une machine de Turing est vraiment composée de seulement deux parties. C'est un automate fini et une mémoire. Si vous y réfléchissez, la mémoire est nécessaire. Quel que soit le calcul que vous faites, vous devez vous souvenir des résultats partiels. La mémoire dans sa version la plus simple consiste simplement à écrire une

chaîne de caractères sur une bande. L'automate fini est en quelque sorte la chose la plus simple que vous puissiez définir et qui fera une sorte de calcul, en fait vraiment n'importe quel type de calcul. Si vous combinez les deux, vous obtenez la machine de Turing. Elle est donc aussi naturelle de ce point de vue.

P versus NP

Nous arrivons maintenant à un très grand sujet, à savoir le problème P versus NP, l'un des problèmes du Prix du Millénaire. Quel est le problème P versus NP ? Pourquoi ce problème est-il le plus important en informatique théorique ? Quelles seraient les conséquences si $P = NP$? Quels outils envisagez-vous qu'une preuve de $P \neq NP$ devrait nécessiter ?

LOVÁSZ : Eh bien, permettez-moi de revenir à l'époque où j'étais étudiant. J'ai parlé à Tibor Gallai, qui était un éminent théoricien des graphes et mon mentor. Il a dit : Voici deux problèmes de théorie des graphes très simples. "Un graphe a-t-il une correspondance parfaite, c'est-à-dire, les sommets peuvent-ils être appariés de sorte que chaque paire soit reliée par une arête ? L'autre est de savoir si le graphe a un cycle hamiltonien, c'est-à-dire, a-t-il un cycle qui contient tous les noeuds ?"

Le premier problème est essentiellement résolu ; il y a beaucoup de littérature à ce sujet. Quant à l'autre problème, nous n'avons que des résultats superficiels, peut-être des résultats non triviaux, mais toujours très superficiels.

Gallai a dit "eh bien, vous devriez y réfléchir, afin que vous puissiez peut-être trouver une explication.". Malheureusement, je n'ai pas pu trouver d'explication à cela, mais avec mon ami, Péter Gács, nous avons essayé de l'expliquer. Et puis nous sommes partis tous les deux - nous avons obtenu des bourses différentes : Gács est allé à Moscou pendant un an et je suis allé à Nashville, Tennessee, pendant un an. Puis nous sommes revenus et nous voulions tous les deux parler en premier, parce que nous avions tous les deux appris la théorie de P versus NP, qui explique complèment cela. Péter Gács l'a apprise de Leonid Levin à Moscou, et je l'ai apprise en écoutant les discussions qui se déroulaient autour des machines à café lors de conférences.

Le problème d'appariement parfait est dans P et le problème du cycle de Hamilton est NP-complet. Cela expliquait ce qui était vraiment une question difficile. Il était clair que cela allait être un sujet central, et cela a été renforcé par le travail de Karp, prouvant la NP-compétude de nombreux problèmes de tous les jours. Donc, en résumé, les notions de P et NP ont mis de l'ordre là où il y avait un tel chaos auparavant. C'était vraiment écrasant.

WIGDERSON : Le fait que cela mette de l'ordre dans un monde qui semblait assez chaotique est la principale raison pour laquelle ce problème est important. En fait, c'est presque une dichotomie, presque tous les problèmes naturels que nous voulons résoudre sont soit dans P, pour autant que nous le sachions, ou bien ils sont NP-complets. Dans les deux exemples donnés par Lovász, d'abord l'appariement parfait, qui est dans P, nous pouvons le résoudre rapidement, nous pouvons le caractériser et faire beaucoup de choses, nous le comprenons vraiment bien. Le deuxième exemple, le problème du cycle hamiltonien est représentatif d'un problème NP-complet.

Le point principal à propos de la NP-complétude est que chaque problème de cette classe est équivalent à tous les autres. Si vous en résolvez un, vous les avez tous résolus. Nous connaissons maintenant des milliers de problèmes que nous voulons résoudre, en logique, en théorie des nombres, en combinatoire, en optimisation, etc., qui sont équivalents.

Donc, nous avons ces deux classes qui semblent séparées, et la question P versus NP consiste à savoir si elles soient égales ou non ; et tout ce que nous avons besoin de savoir, c'est la réponse à l'un des problèmes NP-complets.

Mais je veux examiner l'importance de ce problème d'un point de vue plus élevé. En rapport avec ce que j'ai dit sur les problèmes naturels que nous voulons calculer, je soutiens souvent dans des conférences de vulgarisation que les problèmes dans NP sont vraiment tous les problèmes que nous, les humains, en particulier les mathématiciens, pouvons espérer résoudre, parce que la chose la plus fondamentale à propos des problèmes que nous essayons de résoudre, c'est que nous saurons, au moins, si nous les avons résolus, n'est-ce pas ? Cela n'est pas seulement vrai pour les mathématiciens. Par exemple, les physiciens n'essaient pas de construire un modèle pour quelque chose dont, lorsqu'ils le trouveront, ils ne sauront pas qu'ils l'ont trouvé. Et il en va de même pour les ingénieurs concepteurs ou les détectives avec des solutions à leurs énigmes. Dans chaque entreprise dans laquelle nous nous embarquons sérieusement, nous supposons que lorsque nous trouvons ce que nous cherchions, nous savons que nous l'avons trouvé. Mais c'est la définition même de NP : un problème est dans NP exactement si vous pouvez vérifier si la solution que vous avez obtenue est correcte.

Alors maintenant, nous savons ce qu'est NP. Si P = NP, cela signifie que tous ces problèmes peuvent être résolus par un algorithme efficace, ils peuvent donc être résolus très rapidement sur un ordinateur. Dans un certain sens, si P = NP, alors tout ce que nous essayons de faire peut être fait. Peut-être trouver un remède contre le cancer ou résoudre d'autres problèmes graves, toutes ces questions peuvent être résolues rapidement par un algorithme. C'est pourquoi P=NP est important et aurait tant de conséquences. Cependant, je pense que la plupart des gens pensent que P≠NP.

LOVÁSZ : Permettez-moi d'ajouter une autre réflexion sur la façon dont il peut être prouvé que P=NP. Il y a ici une belle analogie avec les constructions à la règle et au compas. C'est l'un des algorithmes les plus anciens, mais que pouvez-vous construire avec une règle et un compas ? Les Grecs ont formulé des problèmes concernant la trisection de l'angle et le doublement du cube par la règle et le compas, et ils croyaient probablement, ou conjecturaient, que ceux-ci ne pouvaient pas être résolus par la règle et le compas. Mais le prouver n'est pas facile, même aujourd'hui. Je veux dire, cela peut être enseigné dans une classe de premier cycle, dans une classe de premier cycle avancée, je dirais. Il faut connaître la théorie des nombres algébriques et un peu la théorie de Galois pour pouvoir prouver cela. Donc, prouver que ces problèmes ne peuvent pas être résolus par un algorithme spécifique a nécessité un énorme développement dans un domaine complètement différent des mathématiques.

Je m'attends à ce que P ≠NP soit similaire. Bien sûr, nous n'aurons probablement pas à attendre 2000 ans pour avoir la solution, mais cela nécessitera un développement substantiel dans un domaine dont nous n'avons même pas idée aujourd'hui.

Mais nous tenons pour acquis que vous pensez tous les deux que P est différent de NP, n'est-ce pas ?

WIGDERSON : Oui, mais je dois dire que les raisons que nous avons ne sont pas très fortes. La raison principale est que pour les mathématiciens, il semble évidemment beaucoup plus facile de lire des preuves de théorèmes déjà découverts, que de découvrir ces preuves. Cela suggère que P est différent de NP. De nombreuses personnes ont essayé de trouver des algorithmes pour de nombreux problèmes NP-complets pour des raisons pratiques, par exemple, divers problèmes d'ordonnancement et d'optimisation, des problèmes de théorie des graphes, etc. Et ils ont échoué, et ces échecs peuvent suggérer qu'il n'existe pas de tels algorithmes. Ceci, cependant, est un argument faible.

En d'autres termes, je sens intuitivement que P $\neq$ NP, mais je ne pense pas que ce soit un argument solide. Je le crois juste comme une hypothèse de travail.

Problèmes versus théorie

Nous caractérisons souvent les mathématiciens soit comme des constructeurs de théories soit comme des résolveurs de problèmes. Où vous placeriez-vous sur une échelle allant de constructeur de théories à résolveur de problèmes ?

WIGDERSON : Avant tout, j'aime résoudre des problèmes. Mais alors je me demande : Oh, c'est comme ça que j'ai résolu le problème, mais c'est peut-être une technique qui peut être appliquée à d'autres endroits ? Puis j'essaie de l'appliquer ailleurs, puis je l'écris sous sa forme la plus générale, et c'est ainsi que je le présente. De cette façon, je peux aussi être appelé un constructeur de théorie. Je ne sais pas. Je ne veux pas me caractériser en termes de constructeur de théorie ou de résolveur de problèmes.

J'aime faire les deux choses, trouver des solutions aux problèmes et essayer de comprendre comment elles s'appliquent ailleurs. J'aime comprendre les liens entre différents problèmes, et encore plus entre différents domaines. Je pense que nous avons de la chance en informatique théorique, que tant de domaines apparemment dispersés soient si intimement liés, mais pas toujours de manière évidente, comme avec la difficulté et le hasard. La théorie est construite à partir de telles connexions.

LOVÁSZ : J'ai des sentiments similaires. J'aime résoudre des problèmes. J'ai commencé sous l'inspiration de Paul Erdös, qui décomposait vraiment toujours les questions en problèmes. Je pense que c'était une force particulière de ses mathématiques, qu'il puisse formuler des problèmes simples qui illustraient réellement une théorie sous-jacente. Je ne me souviens plus qui a dit ça de lui : ce serait bien de connaître les théories générales qui sont dans sa tête, qu'il décompose en ces problèmes, dont il nous nourrit pour que nous puissions les résoudre. Et, en effet, sur la base de ses problèmes, de tout nouveaux domaines sont apparus, la théorie des graphes extrêmaux, la théorie des graphes aléatoires, la combinatoire probabiliste en général, et divers domaines de la théorie des nombres. J'ai donc commencé comme résolveur de problèmes, mais j'ai toujours aimé établir des liens et j'ai essayé de construire quelque chose de plus général, à partir d'un problème particulier que j'avais résolu.

Jeunesse à Haïfa

Professeur Wigderson, vous êtes né en 1956 à Haïfa, en Israël. Pouvez-vous nous dire quand vous vous êtes intéressé aux mathématiques et, en particulier, à l'informatique théorique ?

WIGDERSON : Je me suis intéressé aux mathématiques bien plus tôt qu'à l'informatique. En tant que très jeune enfant, mon père m'a initié aux mathématiques. Il aimait me poser des questions et étudier des énigmes, et je m'y suis intéressé. Nous avons trouvé des livres que je pouvais lire, et dans ceux-ci, il y avait plus de problèmes. Ce fut ma principale interaction précoce avec les mathématiques. Au lycée, nous avions un très bon professeur de mathématiques qui venait d'Ukraine, et il avait une classe spéciale pour les enfants intéressés. Il nous a appris des choses plus excitantes, comme des trucs de niveau universitaire, et je devins encore plus excité par les mathématiques. Au collège, je me suis beaucoup plus intéressé à cela, mais c'est en fait par accident que je suis entré dans l'informatique, et donc dans l'informatique théorique.

Après mon service militaire, alors que je postulais dans des universités en Israël, j'ai pensé que je voulais faire des mathématiques, mais mes parents ont suggéré qu'il serait peut-être bon d'avoir aussi une profession quand j'aurais obtenu mon diplôme. Donc ils m'ont dit : "Pourquoi n'étudies-tu pas l'informatique, il y aura probablement beaucoup de mathématiques là-dedans, et de toute façon, ça te plaira. En plus, lorsque tu obtiendras ton diplôme, tu auras un diplôme en informatique." Personne ne pensait au milieu universitaire à ce moment-là.

Je suis donc allé au département d'informatique du Technion, et je pense que j'ai été extrêmement chanceux. Je suis sûr que si j'étais allé dans un département de mathématiques, j'aurais été intéressé par bien d'autres choses, comme l'analyse, la combinatoire, la géométrie, etc. Comme j'étais dans le département d'informatique, j'ai suivi plusieurs cours théoriques. Nous avions notamment un professeur très inspirant, Shimon Even, au Technion. Ses cours sur les algorithmes et la complexité étaient extrêmement inspirants. Quand j'ai postulé à l'école doctorale, j'ai postulé pour continuer à faire ce genre de choses. C'est ainsi que j'ai été attiré par l'informatique théorique.

Mais encore, dans une interview précédente, vous vous êtes décrit comme un gars des plages et un passionné de football. Cela contraste assez fortement avec ce que vous nous dites maintenant, n'est-ce pas ?

WIGDERSON : Je ne pense pas qu'il y ait un contraste. J'ai mentionné que mon père était mon principal contact intellectuel en mathématiques. Les écoles du quartier de notre maison n'étaient pas d'un très bon niveau, c'était assez ennuyeux. Le quartier était situé près de la plage, donc tout le monde était à la plage. Nous étions des amateurs de plage par définition. Le temps en Israël est magnifique, vous pouvez donc passer 300 jours par an sur la plage et dans l'eau. C'était donc une activité passe-temps. L'autre chose que vous avez mentionnée, le football, est le jeu auquel il est le plus facile de jouer. Vous n'avez besoin d'aucune installation. Et c'est ce que nous avons fait, étant impliqués dans ces deux activités. Quand je grandissais, je ne me voyais jamais comme un intellectuel. J'adorais les maths, mais j'adorais aussi le football, j'adorais la natation et j'adorais la lecture. Et c'est ainsi que j'ai passé toute ma jeunesse. Il n'y avait pas de contraste et, au contraire,

c'est probablement bien de faire autre chose.

Jeunesse à Budapest

Professeur Lovázs, vous n'étiez certainement pas un gars des plages.

LOVÁSZ : Quand je suis entré en huitième année, il n'y avait pas de matière scolaire qui m'intéressait particulièrement. En huitième année, j'ai commencé à fréquenter un club de mathématiques et j'ai réalisé combien il y avait de problèmes intéressants. Ensuite, le professeur du club de mathématiques a recommandé que j'aille dans une école secondaire particulière qui venait d'ouvrir et se spécialisait dans l'enseignement aux enfants doués en mathématiques. Nous avions dix cours de mathématiques par semaine, ce que ce groupe d'étudiants appréciait beaucoup, moi y compris. J'ai beaucoup apprécié le fait de faire partie d'un groupe assez important d'étudiants qui avaient des intérêts assez similaires.

Au primaire, j'étais un peu en dehors du groupe "cool" de la classe. Je n'étais pas dans le courant dominant de la classe, mais dans cette nouvelle classe de lycée je me trouvais beaucoup plus chez moi. En fait, je me sentais tellement chez moi que j'ai épousé une de mes camarades de classe, Katalin Vesztergombi, et nous sommes toujours ensemble.

Ce lycée était absolument un bon début pour ma vie, c'est ce que je ressens à ce sujet. Avant cela... il fallait juste survivre à l'école. Je suis entré dans ce nouveau lycée dans la première moitié des années soixante. Il y avait beaucoup de bons mathématiciens à Budapest à cette époque, et ils n'avaient pas vraiment la chance de voyager ou de faire quoi que ce soit en dehors de la Hongrie. Ils avaient donc plus de temps, et ils sont venus au lycée et ont donné des conférences et ils se sont beaucoup intéressés à notre groupe. Nous avons beaucoup appris d'eux. Je devrais, bien sûr, mentionner que Paul Erdös visitait souvent la classe et faisait des exposés et posait des problèmes. Tout cela était donc très inspirant.

Professeur Lovász, pour citer le professeur Wigderson : "Au pays des prodiges et des stars en Hongrie, avec sa tradition de résolution de problèmes, il (c'est-à-dire vous) se démarque. Nous avons un témoin qui se rappelle s'être précipité chez lui depuis l'école pour regarder la finale d'un des concours auxquels vous avez participé à la télévision nationale, où vous avez résolu un problème combinatoire en temps réel et gagné la compétition. C'est un peu difficile d'imaginer faire de telles choses maintenant et à l'Ouest.

LOVÁSZ : Vous avez raison. C'était l'une des choses qui ont duré pendant quelques années à la télévision hongroise, mais malheureusement ça s'est arrêté. Malheureusement, car je trouvais que c'était une très bonne vulgarisation des mathématiques. Vous savez, les gens aiment regarder les compétitions. La façon dont cela fonctionnait était qu'il y avait deux cellules en verre, et les deux étudiants qui concouraient étaient assis dans des cellules séparées. Ils avaient eu le même problème qu'ils devaient résoudre, puis devaient donner verbalement la solution ; peut-être y avait-il un tableau noir qu'ils pouvaient aussi utiliser. Je pense que les gens aiment voir les jeunes transpirer et faire de leur mieux pour gagner. Vous savez, la plupart des gens ne savent pas sauter plus de deux mètres, mais nous regardons quand même les Jeux Olympiques. Aujourd'hui encore, je rencontre

des gens, bien sûr des personnes âgées, qui disent : "Oh, ouais, je t'ai vu à la télé quand tu étais au lycée, et j'étais en huitième année de primaire, et c'était tellement agréable de te regarder." C'était vraiment quelque chose d'assez spécial.

Une partie de cette histoire à la fois drôle et charmante est que vous nous avez dit que la solution au problème final, avec lequel vous avez remporté le concours, vous l'aviez apprise auparavant de l'autre concurrent. Est-ce exact ?

LOVÁSZ : Oui c'est vrai. Mais nous, les compétiteurs, étions aussi de bons amis, et nous sommes toujours de très bons amis. Surtout, les deux personnes avec qui j'ai concouru en demi-finale et en finale, sont de très bons amis à moi. L'un était Miklós Laczkovich. Il est venu avec la preuve de la conjecture de Tarski sur la quadrature du cercle. Et l'autre était Lajos Posa. Il est très connu dans l'enseignement des mathématiques. Il a beaucoup fait pour développer des méthodes d'enseignement aux élèves talentueux.

Avant de quitter ce sujet, il convient également de mentionner que vous avez remporté la médaille d'or trois années de suite 1964-1965-1966 aux Olympiades internationales de mathématiques, alors que vous aviez 16-17-18 ans. Ce sont des résultats impressionnants ! Nous ne connaissons personne qui ait un tel record dans cette compétition.

LOVÁSZ : Merci, mais il y en a d'autres. Quelqu'un l'a gagné cinq fois. Vous pouvez aller sur le site Web de l'Olympiade internationale de mathématiques, et vous y trouverez une liste des réalisations.

Lemme local de Lovász

Professeur Lovász, vous avez publié plusieurs articles - nous pensons à six articles en tout - avec votre mentor Paul Erdös. Nous pensons savoir lequel de ces articles est votre préféré, et vous pouvez nous corriger si nous nous trompons. Une version faible de l'important lemme local dit de Lovász a été prouvée en 1975 dans un article conjoint avec Erdös - c'est l'article que nous avons à l'esprit. Le lemme lui-même est très important comme l'attestent Robin Moser et Gábor Tardos recevant le prix Gödel en 2020 pour leur version algorithmique du lemme local de Lovász. Quoi qu'il en soit, pourriez-vous nous dire en quoi consiste le lemme local de Lovász ?

LOVÁSZ : Ok, je vais essayer. En mathématiques, ou du moins en mathématiques discrètes, vous pouvez formuler presque tout comme ceci : il y a un certain nombre de mauvais événements, et vous voulez tous les éviter. La question est de savoir si vous pouvez donner une condition pour éviter tous ces mauvais événements. La chose la plus fondamentale est que si les probabilités de ces événements totalisent quelque chose de moins qu'un, alors avec une probabilité positive, vous les éviterez tous. C'est une astuce très basique dans les applications des probabilités en mathématiques discrètes. Mais supposons que le nombre soit beaucoup plus grand, de sorte que les probabilités totalisent quelque chose de très grand, comment gérez-vous cela ? Un autre cas particulier conernce le cas où il s'agit d'événements indépendants. Si vous pouvez éviter chacun d'eux séparément, alors il y a une probabilité positive que vous les évitiez tous, prenez simplement le produit des probabilités pour éviter chacun d'eux.

Le lemme local est une sorte de combinaison de ces deux idées. Si les événements ne sont pas indépendants, mais que chacun d'eux ne dépend que d'un petit nombre d'autres, et si la somme des probabilités de ceux dont il dépend est inférieure à un - pas la somme totale, mais seulement ceux dont il dépend - alors vous pouvez toujours, avec une probabilité positive, éviter chacun des mauvais événements.

Je devrais peut-être ajouter une chose ici. Il y avait un problème d'Erdös auquel je pensais, et j'ai trouvé ce lemme. J'étais avec Erdös, en fait à Ohio State pour une université d'été. Nous avons résolu le problème, et nous avons écrit un long article sur ce problème et les problèmes connexes, y compris ce lemme. Mais Erdös s'est rendu compte que ce lemme était plus qu'un simple lemme pour ce problème particulier, et il s'est assuré qu'il soit connu sous mon nom. Normalement, ce lemme devrait s'appeler lemme local d'Erdös-Lovász, car il est apparu dans un de nos articles communs, mais Erdös a toujours promu les jeunes et a toujours voulu s'assurer qu'ils deviennent connus s'ils avaient prouvé quelque chose d'important. J'ai profité de sa générosité.

La conjecture de Kneser

En 1955, Kneser a conjecturé le nombre de couleurs dont vous avez besoin pour colorer un type de graphes naturels, maintenant connus sous le nom de graphes de Kneser. En 1978, vous, Professeur Lovász, avez prouvé cette conjecture en codant le problème comme une question d'espaces de grande dimension, à laquelle vous avez répondu en utilisant un outil standard de la théorie de l'homotopie, et ainsi stimulé le domaine de la topologie combinatoire. Comment une telle ligne d'approche vous est-elle venue, et pouvez-vous dire quelque chose sur le problème et votre solution ?

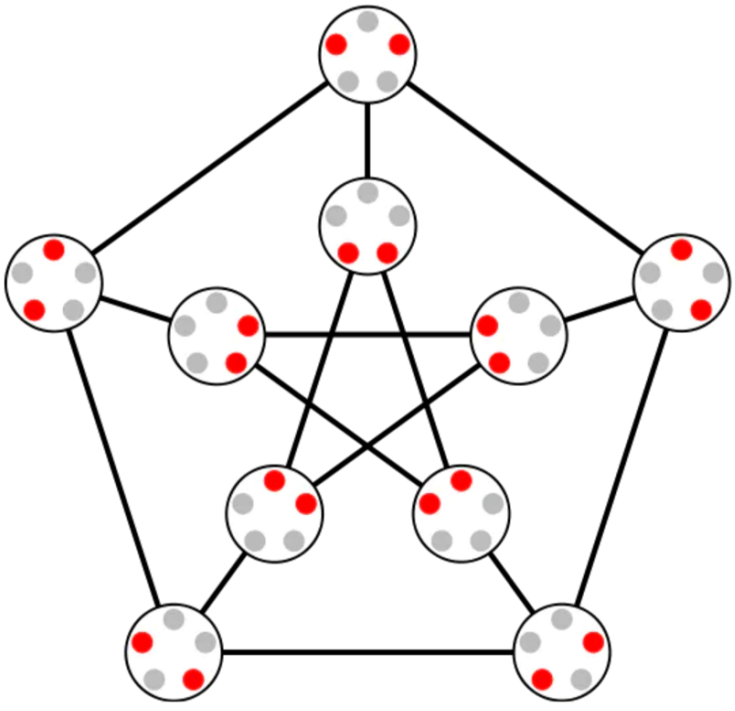

FIGURE 1 : Graphe de Kneser K(5,2)

LOVÁSZ : Cela renvoie à l'un de ces problèmes difficiles, le problème des nombres chromatiques :

combien de couleurs faut-il pour colorer correctement un graphe, où correctement signifie que les sommets voisins doivent avoir des couleurs différentes. C'est un problème difficile en général, c'est un problème NP-complet.

Une première approche consiste à examiner la structure locale. Si un graphe a de nombreux sommets mutuellement adjacents, alors, bien sûr, vous avez besoin de plusieurs couleurs. La question est : y a-t-il toujours une telle structure locale ? On savait déjà à l'époque qu'il existe des graphes qui n'ont absolument aucune structure locale, donc ils n'ont pas de cycles courts, mais il faut quand même beaucoup de couleurs pour les colorer. C'était une question intéressante que de construire de tels graphes. Par exemple, excluez simplement les triangles ou, plus généralement, excluez les cycles impairs du graphe. Il y avait une construction bien connue pour un tel graphe en regardant la sphère, puis en connectant deux points s'ils sont presque antipodaux. Ensuite, le théorème de Borsuk-Ulam dit que vous aurez besoin de plus de couleurs que la dimension, de sorte que les points presque antipodaux aient des couleurs différentes. C'était une construction, et l'autre était la construction où les sommets seraient un sous-ensemble à k éléments d'un ensemble à n éléments, où $n > 2k$ et vous pouvez connecter deux d'entre eux s'ils sont disjoints. Kneser a conjecturé quel serait le nombre chromatique d'un tel graphe.

C'était un problème intéressant qui circulait à Budapest. Simonovits, un ami et collègue à moi, a attiré mon attention sur le fait que ces problèmes pouvaient en fait être similaires, ou que ces deux constructions pouvaient être similaires. J'ai donc proposé une réduction de l'un dans l'autre, mais ensuite il s'est avéré que la réduction était plus générale et donnait une limite inférieure sur les nombres chromatiques de n'importe quel graphe en termes de construction topologique. C'est ainsi que la topologie est apparue. Il a fallu en fait un certain temps pour que cela fonctionne. Si je me souviens bien, j'ai passé environ deux ans à faire fonctionner ces idées, mais finalement cela a fonctionné.

Preuves à divulgation nulle

Professeur Wigderson, plus tôt dans votre carrière, vous avez apporté des contributions fondamentales à un nouveau concept de cryptographie, à savoir la preuve à divulgation nulle, qui plus de 30 ans plus tard est maintenant utilisée par exemple dans la technologie blockchain. Veuillez nous dire précisément ce qu'est une preuve à divulgation nulle et pourquoi ce concept est si utile en cryptographie ?

WIGDERSON : En tant que mathématicien, supposons que vous trouviez la preuve de quelque chose d'important, comme l'hypothèse de Riemann. Et vous voulez convaincre vos collègues que vous avez trouvé cette preuve, mais vous ne voulez pas qu'ils la publient avant vous. Vous voulez les convaincre uniquement du fait que vous avez une preuve de ce théorème, et rien d'autre. Cela semble ridicule, cela semble absolument ridicule, et c'est contraire à toute notre intuition qu'il existe un moyen de convaincre quelqu'un de quelque chose qu'il ne croit pas, sans lui donner la moindre information nouvelle.

Cette idée même a été soulevée par Goldwasser, Micali et Rackoff en 1985, où ils ont suggéré cette notion. Ils ne l'ont pas suggéré pour les mathématiciens paranoïaques, mais ils l'ont suggéré pour

la cryptographie. Ils se sont rendus compte qu'en cryptographie il y a beaucoup de situations, en fait, presque toutes les situations, d'interactions entre agents dans un protocole cryptographique, dans lesquelles personne ne fait confiance aux autres. Néanmoins, chacun d'eux prétend qu'il fait quelque chose, ou qu'il sait quelque chose, qu'il ne veut pas partager avec vous. Par exemple, leur clé privée dans un système cryptographique public. Vous savez, chacun est censé calculer sa clé publique en multipliant deux nombres premiers, qu'il garde secrets. Je vous donne un nombre et je vous dis : voici un nombre ; j'ai multiplié deux nombres premiers secrets et voici le résultat. Pourquoi devriez-vous me croire ? Peut-être que j'ai fait autre chose, et cela va ruiner le protocole. Pour arranger ça, ce serait bien s'il y avait un moyen pour moi de vous convaincre que c'est exactement ce que j'ai fait, à savoir, il existe deux nombres premiers dont le produit est le nombre que je vous ai donné. C'est un théorème mathématique, et je veux vous en convaincre, sans vous donner la moindre idée de ce que sont mes nombres premiers, ni quoi que ce soit d'autre. Goldwasser, Micali et Rackoff ont suggéré cette notion extrêmement utile de preuve à divulgation nulle.

Ils ont donné quelques exemples non triviaux, qui étaient déjà liés à des systèmes cryptographiques existants où cela pourrait être possible. Et ils ont posé la question : pour quel type d'énoncés mathématiques pouvez-vous avoir une preuve à divulgation nulle ? Un an plus tard, avec Goldreich et Micali, nous avons prouvé que c'était possible pour n'importe quel théorème mathématique. Si vous voulez la formulation formelle de cela, c'est vrai pour n'importe quelle NP-énoncé.

Voilà donc le contenu du théorème. Je ne vais pas vous dire la preuve du théorème, bien qu'on puisse en dire quelque chose. La preuve utilise la cryptographie de manière essentielle. C'est un théorème qui suppose la capacité de crypter. Pourquoi c'est utile en cryptographie, c'est exactement pour les raisons que j'ai décrites, mais, en fait, c'est beaucoup plus général, comme nous l'avons observé dans un article ultérieur. Avec une preuve à divulgation nulle, vous pouvez vraiment automatiser la génération de protocoles sûrs contre les mauvais joueurs. La façon d'obtenir un protocole résistant aux mauvais joueurs une fois que vous avez un protocole qui fonctionne si tout le monde est honnête et fait exactement ce qu'il doit, est simplement d'intervenir à chaque étape avec une preuve à divulgation nulle, dans laquelle les joueurs potentiellement mauvais convainquent les autres qu'ils font ce qu'il faut. C'est beaucoup plus complexe, la divulgation zéro ne suffit pas, il faut savoir calculer avec des secrets.

Je tiens à souligner que lorsque nous avons prouvé ce théorème, c'était un résultat théorique. Il était clair pour nous dès le le début que le protocole qui permet la preuve à divulgation nulle est complexe. Nous pensions qu'il était peu probable qu'il soit d'une quelconque utilité dans les protocoles cryptographiques qui s'exécutent sur des machines.

Le fait que ces preuves soient devenues pratiquement utiles est toujours une chose étonnante pour moi, et je pense que c'est un bon point à souligner à propos de nombreux autres résultats théoriques en informatique théorique, en particulier sur les algorithmes. Les gens ont parfois tendance à se plaindre que le fait d'être P soit une condition trop libérale lorsqu'ils décrivent des algorithmes efficaces, car certains algorithmes, lorsqu'ils ont été découverts pour la première fois, peuvent avoir un temps d'exécution qui semble trop grand. C'est du temps polynomial, mais c'est peut-être n à la puissance $10^{\text{ème}}$, et pour n de taille mille, ou de taille un million, qui sont des problèmes qui se posent naturellement dans la pratique, ça semble inutile d'obtenir un algorithme dans P, aussi

inutile qu'obtenir un algorithme à temps exponentiel. Mais ce que vous apprenez encore et encore, à la fois dans le domaine de la cryptographie et dans le domaine des algorithmes, c'est qu'une fois que vous avez une solution théorique avec des idées qui la rendent très efficace, alors d'autres personnes, surtout si elles sont suffisamment motivées, comme en cryptographie ou en optimisation, peuvent la rendre beaucoup plus efficace, et éventuellement pratique. C'est un point général que je voulais faire valoir.

Aléa versus efficacité

C'est un résultat étonnant, et nous vous citons : "C'est probablement le plus surprenant, le plus paradoxal des résultats que mes collègues et moi avons prouvé". Continuons, Professeur Wigderson, avec un autre sujet auquel vous avez apporté une contribution fondamentale. Lorsque vous avez commencé votre carrière universitaire à la fin des années 1970, la théorie de la complexité computationnelle en était à ses balbutiements. Votre contribution à l'élargissement et à l'approfondissement du domaine est sans doute supérieure à celle de toute autre personne. Nous voulons nous concentrer ici sur vos avancées étonnantes dans le rôle du hasard dans l'aide au calcul. Vous avez montré, avec vos collègues Nisan et Impagliazzo, que pour tout algorithme rapide qui peut résoudre un problème difficile en utilisant le retournement de pièces, il existe un algorithme presque aussi rapide qui n'utilise pas le retournement de pièces, à condition que certaines conditions soient remplies. Pourriez-vous développer votre pensée à ce propos ?

WIGDERSON : Le hasard m'a toujours fasciné. Plus précisément, le pouvoir du hasard dans le calcul, mais pas seulement dans le calcul. C'est probablement le domaine où j'ai investi le plus de mon temps de recherche. Je veux dire, un temps de recherche réussi ! Pendant le reste de mon temps qui a consisté à essayer de prouver des limites inférieures ou des résultats sur la difficulté des algorithmes, comme prouver que P est différent de NP, j'ai en général, comme n'importe qui d'autre - échoué.

Donc, retour au hasard. Depuis les années 1970, les gens ont réalisé que le hasard est une ressource extrêmement puissante à utiliser dans les algorithmes. Il y a eu des découvertes initiales, comme des tests de primalité. Solovay/ Strassen et Miller/Rabin ont découvert des méthodes rapides avec un caractère aléatoire pour tester si un nombre est premier. Puis en théorie du codage, en théorie des nombres, en théorie des graphes, en optimisation, etc., le hasard était utilisé partout. Les gens viennent de réaliser que c'est un outil extrêmement puissant pour résoudre des problèmes dont nous n'avons aucune idée de la manière de les résoudre efficacement sans hasard. Avec le hasard, vous pouvez trouver la solution très rapidement. Une autre classe célèbre d'exemples est celle des méthodes de Monte Carlo. Vous explorez donc une grande partie des problèmes en utilisant le hasard. Sans cela, il semblait que cela prendrait un temps exponentiel pour les résoudre, et il était naturel de croire qu'utiliser le hasard est beaucoup plus puissant que de ne pas l'utiliser.

Néanmoins, principalement à partir de motivations en cryptographie, les gens se sont lancés dans la complexité computationnelle en essayant de comprendre le pseudo-aléatoire. Vous avez besoin d'aléatoire dans les protocoles cryptographiques pour le secret. D'un autre côté, parfois, les bits aléatoires n'étaient pas aussi disponibles, et vous vouliez tester quand les bits aléatoires sont bons, ainsi qu'avoir des lancers de pièces indépendants - ce que vous supposez vraiment lorsque vous

parlez d'algorithmes probabilistes.

Donc, il y avait une quête pour comprendre quand une distribution de bits est aussi bonne qu'aléatoire. Cela a commencé en cryptographie avec un travail très puissant de Blum, Micali et Yao. Des notions ont commencé à émerger suggérant que si vous avez une difficulté de calcul, si vous avez d'une manière ou d'une autre un problème difficile, alors vous pouvez générer des bits pseudo-aléatoires à moindre coût. On peut donc investir beaucoup moins d'aléatoire pour générer beaucoup, ce qui reste utile, disons pour des algorithmes probabilistes.

Ce type de compréhension a commencé au début des années 1980. Il a fallu environ 20 ans de travail pour vraiment l'élucider et pouvoir faire les hypothèses les plus faibles sur la difficulté algorithmique dont vous avez besoin pour avoir un résultat pseudo-aléatoire, qui correspond alors à un algorithme probabiliste complet. Des parties de cela ont en effet été développées dans mes articles avec Nisan, puis avec Babai et Fortnow, puis avec Impagliazzo et Kabanets.

Le résultat de ce développement est encore une fois un résultat conditionnel, n'est-ce pas ? Vous devez supposer quelque chose, si vous voulez la conclusion que vous avez énoncée. Ce que vous devez supposer, c'est que certains problèmes sont difficiles. Vous pouvez considérer qu'il s'agit du problème de la coloration des graphes, vous pouvez considérer qu'il s'agit de n'importe quel problème NP-complet que vous aimez, ou même des problèmes qui sont d'une difficulté plus élevée, mais vous avez besoin d'un problème qui est exponentiellement difficile. C'est l'hypothèse sur laquelle le résultat est conditionné. Si vous êtes prêt à faire cette hypothèse, alors la conclusion est exactement comme vous l'avez dit, à savoir que tout algorithme probabiliste efficace peut être remplacé par un algorithme déterministe qui fait la même chose. En fait, il le fait sans erreur et est à peu près aussi efficace que l'original.

En d'autres termes, la puissance des algorithmes probabilistes n'est que le fruit de notre imagination. C'est seulement que nous sommes incapables de trouver des algorithmes déterministes dont nous pouvons prouver qu'ils sont aussi efficaces. Ce résultat suggère qu'une telle puissance n'existe pas et que le caractère aléatoire n'aide pas à rendre les algorithmes efficaces plus efficaces.

L'hypothèse sur la difficulté que vous devez faire, était-ce quelque chose à quoi vous vous attendiez ?

WIGDERSON : On s'y attendait complètement ! Tout d'abord, on s'y attendait dans le sens où ils étaient là depuis le début, en particulier dans les travaux de Blum, Micali et Yao que j'ai mentionnés, qui créent des générateurs pseudo-aléatoires qui sont bons contre des algorithmes efficaces et qui supposent des hypothèses de difficulté spécifiques comme ceux utilisés en cryptographie. Par exemple, que la factorisation est difficile ou que des fonctions à sens unique existent. Il s'agit d'hypothèses de difficulté très spécifiques et il est peu probable que ces problèmes soient NP-complets.

Dans mon article avec Nisan, nous avons réalisé qu'une hypothèse beaucoup plus faible est suffisante. Il ne suffisait pas de donner le résultat indiqué à la fin, car ce n'est pas assez efficace, mais cela nous a déjà fait comprendre que les algorithmes aléatoires ne sont pas aussi puissants qu'ils le semblent. Cela n'a pas donné la conséquence BPP=P, qui est la dernière conséquence.

Ce n'était pas surprenant, le paradigme de connexion entre la difficulté et le hasard est venu des toutes premières études de calcul du pseudo-aléatoire, et, si je me souviens bien, de l'article de Blum et Micali, ou peut-être même du doctorat. La thèse de Silvio Micali, s'intitule *Hardness vs. Randomness*. Il y a là une connexion intime - elle était là depuis le début - et la question est de savoir à quel point cette connexion est ténue.

Je devrais probablement mentionner que la conséquence de ce dont nous venons de parler est que la difficulté implique une dérandomisation, et la question est de savoir si cela fonctionne en arrière également. Si vous avez un bon générateur pseudo-aléatoire, ou si vous pouviez dérandomiser tous les algorithmes probabilistes, cela signifie-t-il que vous pouvez prouver quelque chose comme $P \neq NP$? La réponse est que nous avons des résultats partiels comme celui-là. Mon article avec Impagliazzo et Kabanets en est un, et il y a un autre article d'eux deux seulement. Il y a donc des résultats partiels pour l'inverse, et nous ne les comprenons pas entièrement. Mais c'est un lien fascinant, car ces deux questions semblent distinctes l'une de l'autre. Je pense que c'est une découverte très fondamentale du domaine, ce lien intime entre la difficulté de calcul et la puissance du hasard.

L'algorithme LLL

Professeur Lovász, nous voudrions parler de l'algorithme LLL*, un algorithme qui a des applications surprenantes. Par exemple, on prétend que les seuls systèmes cryptographiques capables de résister à une attaque par un ordinateur quantique utilisent* LLL*. L'algorithme apparaît dans votre article avec les frères Lenstra sur la factorisation des polynômes, qui suit plus ou moins le chemin attendu de réduction modulo des nombres premiers, puis en utilisant le lemme de Hensel. Mais d'après ce que nous comprenons, votre percée avec les frères Lenstra était que vous pouviez faire le lien en en temps polynomial par un algorithme vous donnant une approximation du vecteur le plus court dans un réseau. Dites-nous d'abord comment la collaboration avec les frères Lenstra est née.*

Lovász : C'est une histoire intéressante sur les mathématiques et le rôle de la beauté, ou du moins de l'élégance, dans les mathématiques. Avec Martin Grötschel et Alexander Schrijver, nous travaillions sur des applications de la méthode de l'ellipsoïde en optimisation combinatoire. Nous avons proposé un théorème général qui énonce une certaine équivalence de séparation et d'optimisation. En fait, il y avait des problèmes en temps polynomial équivalents, sous certaines conditions supplémentaires légères. Mais il y avait un cas où l'algorithme ne fonctionnait pas, et c'était lorsque le corps convexe se trouvait dans un sous-espace linéaire de dimension inférieure. On pouvait toujours contourner cela, parfois par des méthodes mathématiques, par exemple, en plaçant tout dans un espace de dimension supérieure. Mais il y avait toujours une astuce impliquée que nous voulions éviter.

À un moment donné, j'ai réalisé que nous pouvions résoudre ce problème si nous pouvions résoudre algorithmiquement un problème mathématique très ancien. C'était le résultat de Dirichlet selon lequel plusieurs nombres réels peuvent être approchés simultanément par des nombres rationnels avec le même dénominateur, et la question était de savoir si vous pouviez résoudre ce problème de manière algorithmique. Maintenant on regarde la preuve et on voit tout de suite que la preuve est le contraire d'être algorithmique ; c'est une preuve utilisant le principe des tiroirs, donc cela montre

simplement l'existence d'une telle approximation. Après quelques essais et erreurs, j'ai trouvé un algorithme qui calculait en fait en temps polynomial une telle approximation avec des nombres rationnels avec un dénominateur commun.

Un peu plus tôt, j'avais entendu parler de Hendrik Lenstra, où il parlait de problèmes similaires, mais en termes de treillis et de réduction de bases dans les treillis. Il est maintenant facile de réduire le problème de Dirichlet à un problème de vecteur le plus court d'un réseau. Alors je leur ai écrit, et il s'est avéré que si je pouvais résoudre le problème de Dirichlet, alors ils pourraient factoriser des polynômes en temps polynomial.

C'était en fait très surprenant. On pourrait penser que factoriser un entier devrait être plus facile que de factoriser un polynôme. Mais il s'avère que c'est l'inverse, les polynômes peuvent être factorisés en temps polynomial. C'est ainsi qu'est né cet article conjoint. Puis, quelques années plus tard, Lagarias et Odlyzko ont découvert que cet algorithme pouvait être utilisé pour casser le système appelé syst'—eme crypto du sac à dos. Depuis lors, cet algorithme est beaucoup utilisé pour vérifier la sécurité de divers systèmes cryptographiques.

Pour autant que nous comprenions, il a des applications bien au-delà de tout ce que vous avez imaginé ?

Lovász : Oui définitivement. Par exemple, peu de temps après sa publication, il a été utilisé par Andrew Odlyzko et Herman te Riele dans un calcul numérique très étendu pour réfuter la soi-disant conjecture de Mertens sur la fonction ζ dans la théorie des nombres premiers. Mais le point que je veux souligner est que tout a commencé à partir de quelque chose qui n'était apparemment pas si important. Grötschel, Schriver et moi voulions juste obtenir le meilleur théorème possible sur l'équivalence de l'optimisation et de la séparation. C'était cependant la motivation pour prouver quelque chose qui s'est avéré être très important.

La méthode de l'ellipsoïde

En effet, vous avez publié en 1981 un article avec les coauteurs Grötschel et Schrijver intitulé "La méthode de l'ellipsoïde et ses conséquences en optimisation combinatoire", article largement cité, et que vous avez évoqué dans votre réponse précédente. Il y a une préhistoire à cela, à savoir un article d'un chercheur russe, Khachiyan, contenant un résultat considéré comme sensationnel. Pourriez-vous commenter cela, et comment votre article conjoint est lié au sien ?

Lovász : Khachiyan a donné le premier algorithme en temps polynomial pour la programmation linéaire en utilisant ce qu'on appelle aujourd'hui la méthode de l'ellipsoïde. Je dois dire qu'à l'époque en Union soviétique, il y avait plusieurs autres personnes qui ont travaillé sur des résultats similaires, mais il a prouvé les détails nécessaires. C'est donc Khachiyan qui a prouvé que la programmation linéaire peut être résolue en temps polynomial.

Bien sûr, tout le monde était intéressé. Avant cela, dans la théorie des algorithmes, il existait ces problèmes mystérieux qui, en pratique, pouvaient toujours être résolus efficacement, mais il n'y avait pas d'algorithme en temps polynomial connu pour eux. Alors on s'y est intéressé, et on s'est

rendu compte que pour appliquer la méthode de Khachyian, il n'est pas nécessaire d'avoir une description explicite du programme linéaire. Il est suffisant que le programme linéaire soit donné de telle manière que si vous demandez si un point est un point faisable, alors vous devriez pouvoir le dire, et vous devriez pouvoir les trouver si des contraintes sont violées. Cette observation a été faite par plusieurs personnes, dont Karp et Papadimitriou, et je pense Padberg et Rao. Nous avons réalisé qu'en optimisation combinatoire, il existe de nombreuses situations comme celle-ci.

Ensuite, j'ai rencontré Martin Grötschel, et il a trouvé un moyen d'appliquer ces méthodes à un autre vieux problème, à savoir trouver le nombre chromatique d'un graphe parfait en temps polynomial, qui était également un problème non résolu à l'époque. Et pour cela il s'est avéré qu'il fallait appliquer cette méthode ellipsoïdale, non seulement aux programmes linéaires, mais plus généralement aux programmes convexes. Nous avons travaillé dessus avec Lex Schrijver, qui a visité l'Université de Szeged pendant un an où nous avons partagé un bureau, et on a commencé à voir ce qui se passe en général dans l'optimisation convexe et comment l'appliquer. C'est ainsi que nous sommes arrivés à ce résultat que j'évoquais, l'équivalence de la séparation et de l'optimisation, c'était en quelque sorte le résultat principal de cette étude. Finalement, nous avons écrit une monographie sur ce sujet.

Le produit zigzag

Les graphes expanseurs ont été un thème récurrent pour le prix Abel. L'année dernière, nous avons eu Margulis, qui a construit les premiers graphes expanseurs explicites, après que Pinsker eut prouvé qu'ils existaient. Gromov, qui a remporté le prix Abel en 2009, a utilisé des expanseurs sur les graphes de Cayley de groupes fondamentaux, qui étaient pertinents pour l'étude de la conjecture de Baum-Connes. Aussi Szemerédi, qui a remporté le prix Abel en 2012, a utilisé des graphes d'expansion. En 2000, vous, Professeur Wigderson, avec Reingold et Vadhan, avez présenté le produit en zigzag de graphes réguliers, qui est, pour autant que nous comprenions, analogue au produit semi-direct en théorie des groupes, par lequel vous avez donné des constructions explicites d'expanseurs très grands et simples. Pourrions-nous commencer par demander : qu'est-ce que le zig et qu'est-ce que le zag ?

WIGDERSON : Alors, peut-être devrais-je commencer par ce qu'est un graphe d'expansion ? Vous devriez penser aux réseaux, et vous devriez penser que l'une des propriétés souhaitables des réseaux est qu'il y ait une sorte de tolérance aux pannes. Si certaines des connexions sont coupées, vous pourrez toujours communiquer. Il peut s'agir de réseaux informatiques ou de réseaux de routes que vous aimeriez voir hautement connectés. Bien sûr, vous ne voulez pas payer trop cher, donc vous voudriez que ces réseaux soient clairsemés, c'est-à-dire que vous voudriez qu'ils n'aient pas trop de connexions. Vous voulez un grand graphe dans lequel le degré de chaque sommet - c'est-à-dire le nombre de connexions à chaque sommet - est petit, disons constant, par exemple dix.

Un graphe aléatoire aura cette propriété, et toute la question - c'est ce que Pinsker a réalisé - devient : pouvez-vous décrire de tels graphes, et pouvez-vous les trouver efficacement ? Margulis a donné la première construction utilisant ce concept algébrique profond, à savoir la propriété de Kazhdan (T). Ils peuvent également être construits en utilisant les résultats de Selberg et d'autres.

Ensuite, les gens ont commencé à simplifier les preuves. Au moment où j'enseignais cette matière, il y avait des preuves raisonnablement simples, comme celle donnée par Jimbo et Maruoka, et vous pouviez l'enseigner dans une classe en une heure ou deux ; c'est simplement une transformée de Fourier sur des groupes finis. Vous avez donc tout ce que vous voulez, vous avez une très belle construction explicite, vous pouvez même le prouver dans une classe pour les étudiants de premier cycle, mais pour moi, c'était, comme pour de nombreuses preuves basées sur l'algèbre, si mystérieux. Je veux dire, que se passe-t-il ? Qu'y a-t-il vraiment derrière le fait que ce sont des graphes hautement connexes ? C'était une sorte d'obsession pour moi pendant des années, et je ne savais pas quoi en faire.

En 2000, juste après mon arrivée à l'IAS, j'avais deux postdocs ici, Salil Vadhan et Omar Reingold. Nous travaillions sur un projet complètement différent sur le pseudo-aléatoire, où une notion importante est la notion d'extracteur, qui a quelque chose à voir avec la purification du hasard. Je n'en parlerai pas maintenant, mais nous essayions de construire de meilleurs extracteurs. Ce faisant, nous avons réalisé que l'une de nos constructions pouvait être utile pour créer des expanseurs. Les constructions dans le secteur des extracteurs sont souvent itératives, et elles ont une nature combinatoire très différente de celle des constructions, disons, de type algébrique. Une fois que nous avons réalisé cela, nous avons compris que nous avions une construction combinatoire complètement différente des expanseurs, mais plus que cela, une construction dans laquelle, pour moi, la raison pour laquelle ces graphes se développent était évident à partir de la preuve.

C'est le résultat zigzag ; le nom de zigzag a en fait été suggéré par Peter Winkler. La construction commence par un petit graphe qui se développe, et on l'utilise pour continuer à booster un autre graphe pour qu'il devienne un expanseur. Donc, vous branchez ce petit graphe d'une manière ou d'une autre, et vous obtenez un plus grand expanseur, puis vous répétez cela pour en obtenir un plus grand, et ainsi de suite. Ainsi, vous pouvez générer de grands expanseurs arbitraires. Cette construction locale a une image en zigzag si vous la regardez, mais ce n'est pas la chose importante.

Il existe une autre façon de décrire un expanseur qui, je pense, est plus intuitive. Un expanseur est un graphe tel que je pense que c'est plus intuitif. Un expanseur est un graphe tel que, quelle que soit la distribution que vous avez sur les sommets, si vous prenez un sommet de cette distribution et que vous passez de ce sommet à un voisin aléatoire, l'entropie de la distribution augmente. C'est une autre façon de décrire les expanseurs, et cela se voit presque à l'œil nu dans la construction en zigzag. Vous voyez comment l'entropie augmente, et c'est ce que j'aime dans cette façon de voir les choses.

Pour essayer d'avoir une image de ce qui se passe : pour autant que nous comprenions, vous avez un graphe et vous placez cet autre graphe à tous les sommets. Ensuite, vous devez décider comment mettre les bords. Ensuite, essentiellement ce que vous êtes en train de faire, tout comme dans la situation du produit semi-direct où vous avez la règle de multiplication, vous vous déplacez un peu dans l'un des sommets, puis vous sautez jusqu'au sommet suivant, puis vous faites le saut similaire là-bas. Est-ce correct, vaguement ?

Wigderson : C'est tout à fait exact, et d'ailleurs la connexion aux produits semi-directs était quelque chose que nous avons réalisé deux ou trois ans plus tard avec Alexander Lubotzky et Noga

Alon. C'était une sorte de challenge que j'ai ressenti très tôt, à savoir que les graphes qu'on obtenait étaient des expanseurs, ils étaient générés combinatoirement, on les comprenait, et je me demandais si notre construction pouvait être utile pour construire des graphes de Cayley. Et puis avec Noga Alon et Alexander Lubotzky, nous avons réalisé que ce n'était pas seulement similaire, mais que le produit en zigzag est une généralisation combinatoire des produits semi-directs de groupes appliqués aux graphes de Cayley. Il est plus général et se spécialise dans le cas des graphes de Cayley aux produits semi-directs. Par exemple, à cause de cela, vous pouvez prouver que les graphes de Cayley de groupes qui ne sont pas simples peuvent se développer avec un nombre constant de générateurs. Aucune méthode algébrique n'est connue pour donner cela.

Cela a été largement utilisé dans de nombreuses situations, et l'une des choses qu'il faudrait peut-être mentionner est que le espace logarithmique symétrique et le espace logarithmique sont les mêmes, comme l'a montré Reingold en 2004. Cela semble être une idée qui a vraiment fait son chemin. L'utilisez-vous encore vous-même ou avez-vous laissé votre "bébé" grandir et entrer dans la communauté mathématique ?

WIGDERSON : Je pense que c'est formidable que nous ayons une communauté mathématique. Beaucoup de nos idées ont été prises dans des endroits au-delà de mon imagination. Il y a quelque chose de fondamental dans cette construction, et elle a été utilisée comme vous l'avez dit dans ce résultat de Reingold, qui peut plus simplement être décrit comme l'algorithme d'espace logarithmique pour la connexité dans les graphes. En fait, cela remonte à un résultat de Lovász et de ses collaborateurs, et ça peut être considéré comme un résultat de randomisation.

Lovász avec Karp, Aleliunas, Lipton et Rackoff ont montré en 1980 que si vous voulez tester si un grand graphe est connecté, mais que vous n'avez pas de mémoire, vous avez juste besoin de suffisamment de mémoire pour vous souvenir où vous êtes, alors en lançant des pièces, vous pouvez explorer l'ensemble du graphe. Il s'agit de l'algorithme d'espace logarithmique aléatoire pour la connexité des graphes. Dérandomiser cet algorithme était un autre de mes projets que je n'ai jamais pu faire, mais Reingold a observé que si vous prenez le produit zigzag et que vous l'appliquez très intelligemment à leur algorithme randomisé, vous obtenez l'algorithme d'espace logarithmique déterministe pour le même problème. C'est donc un générateur pseudo-aléatoire particulier adapté à cela. Il a également été utilisé dans le nouveau théorème PCP d'Irit Dinur. Donc, oui, il y a quelque chose de général avec ce produit zigzag que d'autres personnes trouvent extrêmement utile.

Influence mutuelle

En fait, cela nous amène à un endroit intéressant de cette interview, car ici nous voyons des liens entre ce que vous faisiez tous les deux.

WIGDERSON : Permettez-moi de mentionner l'une des choses les plus marquantes qui me soient arrivées au cours de mes années post-doctorales. C'était en 1985. J'étais post-doctorant à Berkeley, et il y avait un atelier en Oregon dans lequel Lovász a donné dix conférences. Je ne me souviens pas exactement comment ça s'appelait, mais il y avait des conférences sur l'optimisation, la géométrie des nombres, etc. C'était toute une semaine de conférences et tout le monde voulait entendre le discours de Lovász, et tout le monde appréciait à quel point sa présentation était extrêmement claire.

Mais la chose la plus importante que j'en ai retirée est ce que Lovász a lui-même décrit quand vous lui avez posé la question sur l'algorithme LLL, et sa relation avec le travail sur l'ellipsoïde, etc. Il a souligné comment un point de vue de haut niveau, plutôt qu'un point de vue centré sur un problème spécifique, peut relier de très nombreux domaines des mathématiques de grande importance. Lovász vous a décrit comment une question un peu particulière, notamment le fait d'avoir une solution plus élégante à un problème d'optimisation, a conduit à résoudre le problème de la réduction de base du réseau, et comment cela était lié à l'approximation diophantienne, ainsi que comment cela se connectait à la cryptographie, à la fois pour casser les systèmes cryptographiques et créer des systèmes cryptographiques. Et, vous savez, vous obtenez cette vue panoramique où tout s'accorde avec tout. J'ai été extrêmement influencé par cela, ce fut un événement mémorable incroyable au début de ma carrière.

Lovász : Je pense avoir des souvenirs similaires. La preuveà divulgation nulle était une chose tellement excitante et surprenante que j'ai apprise, et cela m'a en quelque sorte montré à quel point ces nouvelles idées de cryptographie et d'informatique théorique en général étaient puissantes. J'ai toujours été très intéressé par le travail de Wigderson sur le hasard, même si j'essayais parfois d'aller dans la direction opposée et de trouver des exemples où le hasard aide vraiment.

Il faut ajouter que c'est parfois une question de modèle, de modèle de calcul. J'ai mentionné quelques résultats sur l'optimisation convexe, la géométrie convexe, les résultats algorithmiques dans la convexité de haute dimension, et c'est un problème de base de savoir comment vous pouvez calculer le volume si vous avez un corps convexe. Un de mes doctorants des étudiants de l'époque, György Elekes, a proposé une belle preuve montrant qu'il faut un temps exponentiel pour approximer ce volume, même dans un facteur constant. C'était dans notre modèle dans lequel nous avons formulé cette équivalence d'optimisation et de séparation des corps convexes donnée par un oracle de séparation. Quelques années plus tard, et c'est en fait une autre chose que Wigderson a dite, Dyer, Frieze et Kannan ont proposé un algorithme aléatoire pour calculer le volume, ou approximer le volume, en temps polynomial avec une petite erreur relative arbitraire.

La chose intéressante est la dépendance à la dimension. Si la dimension est n alors leur algorithme avait n étapes. Évidemment, c'était très loin d'être pratique, mais cela a lancé leur flot de recherche. J'en ai également fait partie et j'ai vraiment aimé ce résultat, et j'étais assez intéressé par le fait de le rendre plus efficace et de comprendre pourquoi l'exposant est si élevé. Et puis alors l'exposant est bien descendu de 29 à 17, à 10, à 7, à 5, à 4. Il resta longtemps à 4 mais il y a un an, il est descendu à 3. Alors maintenant, l'algorithme est proche d'être pratique. Ce n'est toujours pas le cas, le cube n'est toujours pas suffisant pour que ça soit un algorithme très rapide, mais l'objectif n'est certainement pas ridiculement loin.

Deux commentaires sur cet exemple. Premièrement, comme il s'agit d'un modèle de calcul différent, il est prouvé que le caractère aléatoire aide. Il est prouvé que sans le hasard, cela prend un temps exponentiel, et avec le hasard, il s'agit maintenant d'un temps polynomial décent. Et le second commentaire est que le temps polynomial est un indicateur que ce problème a une structure profonde. Vous explorez cette structure profonde et vous pouvez éventuellement améliorer le temps polynomial en quelque chose de décent.

Graphons

Voici une question pour vous, Professeur Lovász, sur un sujet auquel vous avez apporté des contributions majeures : qu'est-ce que la théorie des limites pour les graphes, et à quoi servent les limites de graphes ? Expliquez également ce qu'est un graphon.

Lovász : Je vais essayer de ne pas être trop technique. Un graphe est souvent donné par une matrice d'adjacence, vous pouvez donc l'imaginer comme une matrice de 0 et 1. Et maintenant, supposons que le graphe devient de plus en plus gros, et que vous ayez cette séquence de matrices. Nous y pensons toujours comme à des fonctions sur le carré unité, où nous venons découper des petits carrés, chaque carré portant un zéro ou un un. Et maintenant, ces fonctions tendent en quelque sorte vers une fonction sur le carré unité, qui peut être continue, ou, du moins non discrète, et qui est un graphon. Ainsi, par exemple, si le graphe est aléatoire, alors chaque carré vaut aléatoirement un ou zéro, alors il tendra vers un carré gris, c'est-à-dire vers un graphon un demi partout. Ainsi, un graphon est une fonction sur le carré unité, qui est mesurable et symétrique, et il s'avère que vous pouvez définir exactement ce que cela signifie qu'une séquence de graphes converge vers un tel graphon.

Maintenant, de nombreuses propriétés des graphes sont préservées, c'est-à-dire que si tous les graphes de la séquence ont une certaine propriété, alors la limite aura également cette propriété. Par exemple, si tous ces graphes ont un bon écart de valeur propre - une propriété que possèdent les expanseurs - alors la limite aura également un bon écart de valeur propre. On considère ici des graphes denses. Donc, vous regardez cet espace de graphons, et ensuite vous devez prouver - et il y a beaucoup de détails techniques là-dedans - que l'espace des graphons dans une métrique appropriée est compact. C'est très pratique de travailler avec ça, car à partir de là, vous pouvez, par exemple, prendre un paramètre de graphe, disons la densité de triangles. On peut définir dans la limite du graphon quelle est la densité des triangles, puis dans ce graphon limite il y aura un graphon qui minimise cela sous certaines autres conditions.

Vous pouvez donc jouer au jeu habituel auquel vous jouez en analyse, qui étudie le minimum, le minimiseur, puis vous essayez de déterminer s'il s'agit d'un local, puis vous essayez de déterminer s'il s'agit d'un minimum local ou d'un minimum global. Toutes ces choses que vous pouvez faire en analyse, vous pouvez les faire dans ce cadre, et tout cela a une traduction en théorie des graphes.

Il est intéressant de mentionner que le lemme de régularité de Szemerédi est étroitement lié à la topologie des graphons. En particulier, la compacité de l'espace des graphons implique une forme forte du lemme de régularité.

Capacité de Shannon

Professeur Lovász, en 1979, vous avez publié un article largement cité intitulé : "Sur la capacité de Shannon d'un graphe". Dans cet article, vous déterminez la capacité de Shannon du pentagone en introduisant des méthodes mathématiques approfondies. De plus, vous avez prouvé qu'il existe un nombre, maintenant appelé nombre de Lovász, qui peut être calculé en temps polynomial. Le nombre

de Lovász est la borne supérieure de la capacité de Shannon associée à un graphe. Pourriez-vous nous en dire un peu plus à ce sujet et nous expliquer quelle est la capacité de Shannon ?

Lovász : Je ne donnerai pas de définition formelle de ce qu'est la capacité de Shannon, mais vous avez un alphabet et vous envoyez des messages composés des lettres de l'alphabet. Maintenant, certaines lettres portent à confusion ou peuvent être confondues, elles ne sont donc pas clairement distinguées par le destinataire. Vous voulez choisir un plus grand sous-ensemble de mots qui peuvent être envoyés sans risque de confusion. Pour deux mots, il doit y avoir au moins une position où ils se distinguent clairement. Donc si l'alphabet est décrit par les sommets d'un graphe, une arête entre deux lettres signifie que ces deux lettres peuvent être confondues. Shannon a proposé ce modèle, et il a déterminé sa capacité. Si vous envoyez des mots très longs, combien de mots pouvez-vous envoyer sans semer la confusion ? Ce nombre croît de façon exponentielle, et la base de cette fonction exponentielle est la capacité de Shannon.

Le graphe pentagonal a été le premier pour lequel la capacité de Shannon n'était pas connue, et j'ai introduit une technique appelée la représentation orthogonale, qui m'a permis de répondre à cette question.

Ceci est un exemple de l'une de ces choses qui se produisent parfois, à savoir que lorsque vous répondez à une question, tout d'un coup, elle commence à avoir sa propre vie. Par exemple, cette notion a été utilisée pour déterminer le nombre chromatique de graphes parfaits. Dans un tout autre sens, un groupe de physiciens en a récemment trouvé des applications tout à fait intéressantes en physique quantique. Alors, tout d'un coup, vous entendez que quelque chose que vous avez fait a inspiré d'autres personnes à faire quelque chose de vraiment intéressant. C'est très agréable.

La conjecture d'Erdös-Faber-Lovász

Notre dernière question mathématique pour vous, Professeur Lovász, concerne la soi-disant conjecture d'Erdös-Faber-Lovász, une conjecture qui a été posée en 1972. Comment cela s'est-il produit et quelles ont été vos premières pensées en réalisant à quel point il serait difficile de le prouver ? Tout récemment, la conjecture a été prouvée par Kang, Kelly, Kühn, Methuku et Osthus. Nous devons également ajouter qu'apparemment, Erdös considérait ce problème comme l'un de ses trois problèmes combinatoires préférés.

Lovász : Le contexte de ce problème était qu'il y avait eu une réunion en août 1972 à l'Ohio State University, où nous avions discuté de la théorie des hypergraphes, qui commençait tout juste à émerger comme un sujet intéressant. L'idée est qu'au lieu d'avoir un graphe standard où une arête a toujours deux extrémités, vous pouvez plutôt regarder des structures où une arête a trois extrémités, ou cinq extrémités, et ainsi de suite. Ceux-ci sont appelés hypergraphes, et la question était la suivante : étant donné une notion particulière en théorie des graphes, comme le nombre chromatique, la connexité, etc., comment cette notion peut-elle être généralisée aux hypergraphes ?

L'une de ces questions était ce qu'on appelle le nombre chromatique d'arête en théorie des graphes. C'est une variante bien connue du problème du nombre chromatique, dans le cas où vous colorez

les arêtes, pas les sommets, et vous voulez que les arêtes incidentes d'un même sommet aient des couleurs différentes. Et puis vous pouvez poser la même question sur les hypergraphes et vous demander quelle limite supérieure vous pouvez établir sur le nombre de couleurs différentes nécessaires. Nous sommes arrivés à cette observation que dans tous les exemples connus, le nombre de sommets était une limite supérieure du nombre de couleurs nécessaires pour colorer l'hypergraphe.

Quelques semaines après cette réunion à Ohio State, je visitais l'Université du Colorado, Boulder, et Erdös aussi. Puis Faber a donné une fête, et nous avons commencé à discuter de mathématiques, c'est ce que les mathématiciens font habituellement lors de fêtes, et alors nous avons posé cette question.

Erdös ne croyait pas vraiment que cela était vrai. J'étais plus optimiste et j'ai pensé que c'était peut-être vrai. C'était certainement une belle conjecture, indiquant que le nombre de sommets était une limite supérieure du nombre de couleurs nécessaires. Ensuite, nous avons réalisé que la conjecture avait des cas particuliers non triviaux, comme ce qu'on appelle l'inégalité de Fisher dans la théorie de la conception de blocs. Et c'est là que nous nous sommes retrouvés coincés. La conjecture est devenue de plus en plus célèbre, c'est une question très élémentaire, très simple à poser. Personne n'arrivait à la saisir correctement. Finalement, Jeff Kahn a pu, il y a environ 10 ans, la prouver avec un facteur de $1 + \varepsilon$ pour tout ε positif.

Il y a un an, Daniela Kuhn et ses élèves ont pu la prouver, au moins pour tout n assez grand. Une caractéristique particulière de cette conjecture est que vous faites une conjecture basée sur des petits n, et alors vous pouvez la prouver pour n très grand. Et ce qui est entre les deux reste souvent un point d'interrogation. Elle a donné une conférence à ce sujet au Congrès européen il y a quelques mois, et c'était très convaincant, donc je pense que c'est maintenant prouvé.

Preuves interactives quantiques

En janvier 2020, cinq personnes, Ji, Natarajan, Vidick, Wright et Yuen ont annoncé qu'elles avaient prouvé un résultat dans la théorie de la complexité quantique qui impliquait une réponse négative au problème d'intégration de Connes dans la théorie de l'algèbre des opérateurs. Cela a été une surprise totale pour beaucoup de gens, y compris nous deux, car nous connaissons un peu le problème de Connes, un problème dont la preuve a résisté à toutes les attaques au cours des quarante dernières années. Qu'un problème qui semble n'avoir rien à voir avec la théorie de la complexité quantique trouve sa solution dans ce dernier domaine nous étonne. Professeur Wigderson, avez-vous des commentaires ?

WIGDERSON : Depuis que ce résultat est sorti, j'ai essayé de donner des conférences populaires sur l'évolution du domaine particulier qui est pertinent pour ce résultat, à savoir les preuves interactives, en particulier l'étude des preuves interactives quantiques et comment elles se connectent au résultat MIP*=RE, ainsi qu'à des questions particulières, comme le problème d'intégration de Connes et le problème de Tsirelson dans la théorie de l'information quantique. Bien sûr, chaque résultat particulier peut être surprenant, mais je ne suis pas du tout surpris par ce lien. À l'heure actuelle, nous avons beaucoup, beaucoup de domaines partout dans les mathématiques où les idées de l'informatique théorique, des algorithmes et, bien sûr, des mathématiques discrètes,

sont présentes et révèlent leur puissance.

Quant à la connexion aux algèbres d'opérateurs, et plus particulièrement aux algèbres de von Neumann, ce n'est pas aussi mystérieux que cela puisse paraître, à cause des mesures quantiques impliquant des applications d'opérateurs. La question de savoir si ces opérateurs commutent est fondamentale dans la compréhension à la fois de la théorie de l'information quantique et de la puissance des preuves interactives quantiques. J'étais plus concentré sur la raison pour laquelle une preuve pourrait éventuellement être obtenue dans le domaine des preuves interactives quantiques, et non dans la théorie classique de l'information quantique.

Si vous regardez la formulation des preuves interactives quantiques - en particulier celles MIP* des prouveurs multiples - et que vous les comparez à l'article EPR, la célèbre expérience d'Einstein-Podolsky-Rosen Gedanken testant la mécanique quantique, vous voyez la même image. Vous y voyez une preuve interactive à deux prouveurs comme vous le voyez dans les preuves interactives quantiques plus récentes en théorie de la complexité. Si vous regardez l'histoire de l'étude de telles expériences ou preuves, dans le monde de la physique, l'accent était mis sur différents types de problèmes particuliers. Il en existe plusieurs qui sont célèbres, comme les inégalités de Bell. Pourtant, c'est très naturel pour les personnes qui étudient les preuves interactives quantiques de les étudier comme une collection. Il y a une collection de jeux, certains jeux réductibles les uns aux autres, et la preuve que MIP* = RE est une séquence de réductions étonnantes de réductions et de résultats d'amplifications utilisant diverses techniques de théorie du codage quantique et ainsi de suite, même des techniques PCP. Cette façon de voir les choses selon la théorie de la complexité permet de mieux comprendre comment elles se comportent dans leur ensemble, et je pense que c'est la source de la puissance de cette approche, et les applications viennent du résultat final simplement parce que les objets d'étude sont des opérateurs sur un espace de Hilbert.

Optimisation non commutative

Professeur Wigderson, vous travaillez actuellement sur quelque chose qui nous semble assez différent de ce sur quoi vous travailliez précédemment. Vous l'appelez optimisation non commutative, et il nous semble que vous faites de l'optimisation en présence de symétries de certains groupes non commutatifs, de groupes linéaires généraux et de choses comme ça. Cela semble être un projet vraiment fascinant avec des liens avec de nombreux domaines. Voudriez-vous commenter un peu ce que vous faites ici ?

WIGDERSON : Tout d'abord, c'est tout à fait vrai que c'est très différent de tout ce que j'ai pu faire avant, car il s'agit plus d'algorithmes que de complexité. De plus, cela utilise beaucoup plus de mathématiques que je n'en connaissais auparavant. J'ai donc dû apprendre, et je dois encore apprendre beaucoup plus de mathématiques, en particulier la théorie des invariants, la théorie des représentations et une certaine géométrie algébrique dont je n'avais certainement pas conscience et dont je n'avais jamais eu besoin auparavant.

Cela montre à nouveau l'inter-connexité en mathématiques, en particulier, ce qui est utilisé dans différents domaines des mathématiques afin d'obtenir des algorithmes efficaces, et pour obtenir d'autres résultats en mathématiques discrètes. Cette connexion, bien sûr, va aussi dans l'autre sens

et enrichit ces domaines mathématiques.

Ce projet est parti de quelque chose qui m'est très cher, à savoir le projet de dérandomisation auquel je réfléchis depuis trente ans. L'un des problèmes les plus simples dont nous savons qu'il a un algorithme probabiliste, mais dont nous ne savons pas qu'il a une contrepartie déterministe - je veux dire sans hypothèses - est le test d'identités algébriques. Vous pouvez penser aux identités de Newton entre des polynômes symétriques, vous pouvez penser à l'identité de Vandermonde, il y a beaucoup, beaucoup d'identités algébriques en mathématiques.

Si quelqu'un conjecture une identité algébrique, que faites-vous, comment la vérifiez-vous ? Vous pouvez les considérer comme des polynômes avec de nombreuses variables. Bien sûr, vous ne pouvez pas les développer et comparer les coefficients, car cela prendrait un temps exponentiel puisqu'il existe un nombre exponentiel de coefficients. Eh bien, il existe un moyen probabiliste sûr. Ce que nous faisons, c'est simplement insérer des nombres aléatoires dans les variables, évaluer les polynômes en question et comparer les résultats. Ce sera correct avec une forte probabilité. Il existe donc un algorithme probabiliste rapide pour ce problème de test d'identité polynomiale, et nous ne savons pas s'il en existe un algorithme déterministe rapide.

Il y a une vingtaine d'années, Kabanets et Impagliazzo ont réalisé quelque chose d'absolument fondamental, à savoir que si vous trouviez un algorithme de temps polynomial déterministe pour ce problème, vous auriez prouvé quelque chose comme P différent de NP. L'analogue en théorie de la complexité algébrique est que vous auriez prouvé que le permanent est exponentiellement plus difficile à calculer que le déterminant. Bref, un résultat de difficulté qui fera une percée en informatique et en mathématiques !

Tout d'abord, je voudrais dire que cette déclaration devrait être choquante, car un algorithme rapide implique la difficulté d'un problème différent. Cela implique un résultat de difficulté de calcul, ce qui est étonnant. Même avant ce résultat, c'était un problème fondamental d'essayer de dérandomiser, et il y a eu diverses tentatives dans de nombreux cas particuliers sur lesquels j'ai travaillé et d'autres ont travaillé. Et, bien sûr, ce résultat a rendu ces tentatives beaucoup plus importantes.

Il y a quelques années, la question de savoir ce qui se passe avec les polynômes ou les fonctions rationnelles dont vous essayez de prouver qu'elles sont équivalentes, ne concerne pas les variables commutatives, mais plutôt les variables non commutatives. Il est devenu évident que nous en avions besoin dans un projet ici avec deux postdoctorants, Pavel Hrubes et Amir Yehudayoff. Nous avons commencé à travailler sur la version non commutative du test des identités algébriques ; c'est essentiellement le problème de mot pour les champs asymétriques, donc c'est un problème très basique. Il est ressorti de nos tentatives que la théorie des invariants était absolument cruciale pour ce problème. Ainsi, comprendre les invariants de certaines actions de groupe sur un ensemble de matrices, ainsi que comprendre le degré des invariants générateurs de telles actions, est devenu essentiel.

J'ai donc commencé à apprendre à ce sujet et j'ai continué à demander aux gens de ce domaine, puis j'ai commencé à collaborer avec deux étudiants de Princeton, Ankit Garg et Rafael Oliveira.

Finalement, pour faire court, avec Leonid Gurvits, nous avons trouvé un algorithme en temps polynomial déterministe pour résoudre ce problème dans le domaine non commutatif, pour des variables non commutatives. Rien de tel n'était connu, même un algorithme randomisé n'était pas connu, et il utilise essentiellement des résultats dans la théorie des invariants.

Et puis nous avons essayé de comprendre ce que nous faisions. Au cours des cinq dernières années, j'ai tenté à plusieurs reprises de mieux comprendre ce que nous faisions, de comprendre l'étendue de la puissance de ces types d'algorithmes. Quels sont les problèmes auxquels ils sont liés ou peuvent résoudre, et que peuvent faire ces techniques, et quelle est, en général, la signification de ce résultat ?

Je devrais dire quelque chose sur les applications de ce résultat. Il s'avère qu'il capture beaucoup de choses qui semblaient sans rapport. Il est utile non seulement pour tester les identités, mais aussi pour tester les inégalités, comme les inégalités de Brascamp-Lieb. C'est bon pour des problèmes en théorie de l'information quantique, c'est bon pour des problèmes en statistiques, pour des problèmes de théorie des opérateurs. Il semble être très large.

Maintenant, tous ces algorithmes évoluent simplement le long de l'orbite d'une action de groupe sur un espace linéaire. C'est la nature de chacun d'eux. Beaucoup de ces problèmes que nous examinons ne sont pas convexes, donc les méthodes d'optimisation convexe standard ne fonctionnent pas pour eux. Mais ces algorithmes fonctionnent. Et ce que nous avons compris, c'est que ces algorithmes peuvent être considérés comme faisant des optimisations convexes, des méthodes standard du premier ordre et du second ordre, qui sont utilisées dans l'optimisation convexe, sauf qu'au lieu de se dérouler dans l'espace euclidien, ils se déroulent dans une variété riemannienne, et la convexité dont vous avez besoin est la convexité géodésique de cet espace.

Nous avons maintenant une théorie de ces algorithmes, mais, bien sûr, il y en a beaucoup que nous ne comprenons pas. Je trouve le nombre croissant de domaines d'application de cela très fascinant. Bien sûr, j'espère que cela nous aidera finalement à résoudre le cas commutatif et à comprendre ce qui fonctionne et ce qui ne fonctionne pas dans tel ou tel cas.

LL et AW sont des super héros

Pour notre plus grand plaisir également, certains jeunes coréens ont découvert que vous êtes des super-héros mathématiques. Vos deux fils ont leur tuteur de thèse en commun à Stanford, Jacob Fox, et cela a été repris par une revue scientifique populaire sud-coréenne destinée à un public plus jeune, où vous et vos fils êtes représentés comme divers personnages de Star Wars. En tant que scientifiques de haut niveau, vous sentez-vous à l'aise d'être de vrais héros avec des sabres laser et autre ?

Lovász : J'aime toujours une bonne blague, donc je pense que c'était un bon dessin animé.

Wigderson : J'ai aussi adoré, et je pense que cela montre simplement que l'on peut toujours être plus créatif pour susciter l'intérêt du jeune public pour les mathématiques, d'une manière à laquelle on ne s'attendait pas auparavant.

La science est-elle sous pression ?

Il y a une question que nous voudrions poser qui n'a rien à voir en tant que telle avec les mathématiques, et c'est : pensez-vous que la science soit sous pression et est-ce un problème sur lequel les mathématiciens peuvent et doivent s'engager ?

Lovász : Je pense que c'est vrai, la science est sous pression. La raison fondamentale de cela, d'après ce que je vois, c'est qu'elle s'est développée très rapidement, et les gens comprennent de moins en moins ce qui se passe dans chaque science particulière, et cela la rend effrayante, cela la rend étrangère. De plus, cela rend également plus difficile la distinction entre ce qu'il faut croire et ce qu'il ne faut pas, la distinction entre la science et la pseudoscience. Ceci est un vrai problème. Je pense que nous devons repenser très attentivement la façon dont nous enseignons aux élèves du secondaire. Or, les mathématiques font partie des domaines où leur enseignement n'est vraiment pas à la hauteur de ce qu'il pourrait être. Je suppose qu'environ 90 % des personnes que je rencontre disent : "J'ai toujours détesté les mathématiques.".

Je pense que nous ne faisons pas bien notre travail d'enseignement. Je dis cela malgré le fait que certains de mes meilleurs amis travaillent à essayer d'améliorer l'enseignement des mathématiques. Beaucoup de gens se rendent compte qu'il y a un problème à ce niveau, mais c'est très difficile d'aller de l'avant. J'ai moins d'expérience dans d'autres domaines, mais en regardant de l'extérieur, je peux voir à quel point la biologie d'aujourd'hui est différente de ce que j'ai étudié en biologie au lycée. Il est clair que c'est là une tâche énorme devant la communauté scientifique.

Les mathématiques devraient jouer un rôle central parce que beaucoup de sciences utilisent de plus en plus les mathématiques, et non seulement les statistiques, ce qui est en quelque sorte la norme. Par exemple, la théorie des réseaux ou, bien sûr, l'analyse et les équations différentielles, et la physique quantique, qui est vraiment aussi des mathématiques ; c'est un domaine compliqué de l'algèbre multilinéaire, pour ainsi dire. Je pense que le problème est là et qu'il faut faire quelque chose.

Au nom de la Société mathématique norvégienne et de la Société mathématique européenne, et de nous deux, nous voudrions vous remercier pour cette interview très intéressante, et encore une fois, félicitations pour avoir reçu le prix Abel !

Lovász : Merci !

Wigderson : Merci !