THE ABEL PRIZE 2021

L'Académie des sciences et des lettres de Norvège a décidé de décerner le prix Abel 2021 à

László Lovász

de l'université Eötvös Loránd à Budapest, en Hongrie et à

Avi Wigderson

de l'Institute for Advanced Study de Princeton, aux États-Unis,

« pour leurs contributions fondamentales à l'informatique théorique et aux mathématiques discrètes, et pour leur rôle de premier plan dans leur transformation en domaines centraux des mathématiques contemporaines ».

L'informatique théorique est l'étude de la puissance et des limites du calcul. Elle trouve son origine dans les travaux fondateurs de Kurt Gödel, Alonzo Church, Alan Turing et John von Neumann, qui ont conduit au développement de véritables ordinateurs physiques. L'informatique théorique comprend deux sous-disciplines complémentaires : l'algorithmique qui développe des méthodes efficaces pour une multitude de problèmes de calcul ; et la complexité, qui montre les limites inhérentes à l'efficacité des algorithmes. La notion d'algorithmes en temps polynomial mise en avant dans les années 1960 par Alan Cobham, Jack Edmonds et d'autres, ainsi que la célèbre conjecture P≠NP de Stephen Cook, Leonid Levin et Richard Karp ont eu un fort impact sur le domaine et sur les travaux de Lovász et Wigderson.

Indépendamment de son impact considérable sur l'informatique en général et sur sa pratique, l'informatique théorique fournit les bases de la cryptographie, et a maintenant une influence croissante sur plusieurs autres sciences, ce qui permet de faire de nouvelles découvertes en « chaussant des lunettes d'informaticien ». Les structures discrètes telles que les graphes, les chaînes de caractères et les permutations sont au cœur de l'informatique théorique, et les mathématiques discrètes et l'informatique théorique ont naturellement été des domaines étroitement liés. Certes, ces deux domaines ont énormément bénéficié des champs de recherche plus traditionnels des mathématiques, mais on constate également une influence croissante dans le sens inverse. Les applications, concepts et techniques de l'informatique théorique ont généré de nouveaux défis, ouvert de nouvelles directions de recherche et résolu d'importants problèmes ouverts en mathématiques pures et appliquées.

László Lovász et Avi Wigderson ont joué un rôle clé dans cette évolution au cours des dernières décennies. Leurs travaux sont imbriqués de

nombreuses manières et, en particulier, ils ont tous deux apporté des contributions fondamentales à la compréhension de l'aléa dans le calcul et à l'exploration des limites du calcul efficace.

En collaboration avec Arjen Lenstra et Hendrik Lenstra, László Lovász a développé l'algorithme dit LLL de réduction de réseau. Étant donné un réseau euclidien entier de grande dimension, cet algorithme en produit une bonne base, presque orthogonale. En plus de ses nombreuses applications telles qu'un algorithme de factorisation des polynômes rationnels, l'algorithme LLL est l'un des outils préférés des cryptanalystes, et a réussi à casser plusieurs cryptosystèmes proposés. Fait surprenant, l'analyse de l'algorithme LLL est également utilisée pour concevoir et garantir la sécurité de nouveaux cryptosystèmes à base de réseaux euclidiens qui semblent même résister aux attaques des ordinateurs quantiques. Quant à certaines primitives cryptographiques exotiques, telles que le chiffrement homomorphe, les seules constructions connues sont celles de ces cryptosystèmes à base de réseaux euclidiens.

L'algorithme LLL n'est que l'un des nombreux apports visionnaires de Lovász. Il a également prouvé le lemme local, un outil unique pour montrer l'existence d'objets combinatoires dont l'existence est rare, par opposition à la méthode probabiliste standard utilisée lorsque les objets existent en abondance. Aux côtés de Martin Grötschel et de Lex Schrijver, il a montré comment résoudre efficacement des programmes semi-définis, ce qui a conduit à une révolution dans la conception des algorithmes. Il a contribué à la théorie des marches aléatoires avec des applications aux problèmes d'isopérimétrie euclidienne et au calcul du volume approximatif des objets de grande dimension. Son article avec Uriel Feige, Shafi Goldwasser, Shmuel Safra et Mario Szegedy sur les preuves vérifiables en probabilité a donné une première version du théorème PCP, un résultat extrêmement influent montrant que l'exactitude des preuves mathématiques peut être vérifiée de manière probabiliste, avec grande confiance, en ne lisant qu'un petit nombre de symboles ! Par ailleurs, il a également résolu des problèmes de longue date tels que la conjecture du graphe parfait, la conjecture de Kneser, la détermination de la capacité de Shannon du graphe pentagonal, et ces dernières années il a développé la théorie des limites de graphes (en collaboration avec Christian Borgs, Jennifer Chayes, Lex Schrijver, Vera Sós, Balázs Szegedy et Katalin Vesztergombi). Ces travaux relient entre eux des éléments de théorie des graphes extrémaux, de théorie des probabilités et de physique statistique.

Avi Wigderson a largement et profondément contribué à tous les aspects de la complexité, en particulier le rôle du hasard dans le calcul. Un algorithme aléatoire est un algorithme qui tire à pile ou face pour calculer une solution correcte avec probabilité élevée. Au cours des dernières décennies, les chercheurs ont découvert des algorithmes déterministes pour de nombreux problèmes pour lesquels seul un algorithme aléatoire était auparavant connu. L'algorithme déterministe pour les tests de primalité, d'Agrawal, Kayal et Saxena, est un exemple frappant de ce type d'algorithme dérandomisé. Face à ces résultats de dérandomisation, la question se pose de savoir si le hasard est vraiment essentiel. Dans ses travaux avec László Babai, Lance Fortnow, Noam Nisan et Russell Impagliazzo, Wigderson a démontré que la réponse est probablement négative. Formellement, ils ont montré une conjecture de calcul, similaire dans l'esprit à la conjecture P≠NP, qui implique que P=BPP. Autrement dit, chaque algorithme randomisé peut être dérandomisé et transformé en un algorithme déterministe d'une efficacité comparable ; en outre, la dérandomisation est générique et universelle, et ne dépend pas des détails internes de l'algorithme randomisé.

Une autre façon de considérer ce travail est de le voir comme un compromis entre la dureté du calcul et le hasard : s'il existe un problème suffisamment dur, le hasard peut être simulé par des algorithmes déterministes efficaces. Les travaux menés par la suite par Wigderson avec Impagliazzo et Valentine Kabanets prouvent le contraire : des algorithmes déterministes efficaces, même pour des problèmes spécifiques avec des algorithmes aléatoires connus, impliqueraient qu'il doit exister un problème aussi dur.

Ce travail est intimement lié aux constructions d'objets pseudo-aléatoires (c.-à-d. à l'aspect aléatoire). Les travaux de Wigderson ont permis de construire des générateurs pseudo-aléatoires qui transforment quelques bits réellement aléatoires en de nombreux bits pseudo-aléatoires, des extracteurs qui extraient des bits aléatoires presque parfaits d'une source imparfaite d'aléa, des graphes de Ramsey et des graphes expanseurs qui sont creux et qui ont néanmoins une densité élevée. Avec Omer Reingold et Salil Vadhan, il a introduit le produit zigzag de graphes, qui a donné une méthode élémentaire pour construire des graphes expanseurs,

et inspiré la preuve combinatoire du théorème PCP d'Irit Dinur et un algorithme efficace en mémoire pour le problème de densité des graphes de Reingold. Ce dernier explique comment naviguer dans un grand labyrinthe tout en ne se souvenant que de l'identité d'un nombre constant de jonctions du labyrinthe !

Les autres contributions de Wigderson comprennent des preuves à divulgation nulle qui permettent de prouver des affirmations sans révéler d'autre information que la validité des affirmations, et des bornes inférieures sur l'efficacité des protocoles de communication, circuits et systèmes formels de preuve.

Sous l'impulsion de Lovász et Wigderson, les mathématiques discrètes et le domaine relativement jeune de l'informatique théorique sont désormais établis comme des domaines centraux des mathématiques modernes.