Photo credit: Andrea Kane, Institute for Advanced Studies, Princeton, NJ, USA / Abel Prize

Biographie d'Avi Wigderson

Lorsque Avi Wigderson a commencé sa carrière universitaire à la fin des années 1970, la théorie de la « complexité », qui se penche sur la vitesse et l'efficacité des algorithmes, n'en était qu'à ses débuts. A. Wigderson a probablement contribué plus que quiconque à l'élargissement et à l'approfondissement du domaine, et ce qui n'était alors qu'un sujet naissant est devenu aujourd'hui un domaine établi des mathématiques et de l'informatique théorique. La complexité est désormais incroyablement importante, car elle pose les bases théoriques de la sécurité d'Internet.

A. Wigderson est né à Haïfa, en Israël, en 1956. En 1977, il entre à Technion, l'Institut israélien de technologie, et obtient sa licence d'informatique en 1980. Il s'installe à Princeton pour ses études de troisième cycle et obtient son doctorat en 1983 avec la thèse *Studies in Combinatorial Complexity,* sous la direction de Richard Lipton. En 1986, A. Wigderson retourne en Israël pour occuper un poste à l'Université hébraïque de Jérusalem. Il obtient une permanence l'année suivante et devient professeur titulaire en 1991.

Dans les années 1970, les théoriciens de l'informatique ont formulé certaines idées fondamentales sur la nature du calcul, notamment les notions de P et de NP. P représente l'ensemble des problèmes que les ordinateurs peuvent résoudre facilement, par exemple, en quelques secondes, tandis que NP contient également des problèmes durs à résoudre pour les ordinateurs. Autrement dit, des problèmes auxquels les méthodes connues ne permettraient d'apporter une réponse que dans des millions d'années. La question fondamentale de la complexité est de savoir si tous ces problèmes durs peuvent être réduits à des problèmes faciles, c'est-à-dire déterminer si P = NP ou pas. Elle est d'ailleurs aujourd'hui considérée comme l'une des plus grandes questions non résolues dans tout le domaine des mathématiques.

A. Wigderson a réalisé d'incroyables avancées dans ce domaine en étudiant le rôle du hasard dans l'aide au calcul. La dureté de certains problèmes peut être réduite à l'aide d'algorithmes incitant l'ordinateur à tirer à pile ou face pendant le

calcul. Toutefois, lorsqu'un algorithme s'appuie sur le tirage à pile ou face, il y a toujours une chance qu'une erreur puisse se glisser dans la solution. A. Wigderson, d'abord en collaboration avec Noam Nisan, puis avec Russell Impagliazzo, a démontré que pour tout algorithme rapide qui peut résoudre un problème dur grâce au tirage à pile ou face, il existe un algorithme presque aussi rapide qui n'a pas recours à cette méthode, pourvu que certaines conditions soient remplies.

A. Wigderson a mené des recherches sur tous les principaux problèmes ouverts dans la théorie de la complexité. À bien des égards, le domaine s'est développé autour de lui, non seulement en raison de son inlassable curiosité, mais aussi grâce à sa personnalité accessible et son enthousiasme pour les collaborations. Il a co-écrit des articles avec plus de 100 personnes et a accompagné un grand nombre de jeunes théoriciens de la complexité. « Je me considère incroyablement chanceux de vivre à cette époque, déclare-t-il. [La complexité] est un domaine jeune. C'est un domaine très démocratique. C'est un domaine très convivial, c'est un domaine qui est très collaboratif, qui convient à ma nature. Et indéniablement, il regorge de problèmes intellectuels et de défis. »

En 1999, A. Wigderson a rejoint à l'Institute of Advanced Study (IAS) de Princeton où il demeure toujours. Lors d'un événement organisé à l'occasion du soixantième anniversaire de A. Wigderson, en 2016, le directeur de l'IAS, Robbert Dijkgraaf, a déclaré qu'il avait lancé un âge d'or de l'informatique théorique à l'institut.

A. Wigderson est connu pour sa capacité à établir des liens entre des domaines apparemment sans rapport. Il a approfondi les liens entre les mathématiques et l'informatique. Par exemple, le « produit zig-zag de graphes », qu'il a développé avec Omer Reingold et Salil Vadhan, relie la théorie des groupes, la théorie des graphes et la théorie de la complexité, avec des applications surprenantes telles que la meilleure façon de sortir d'un labyrinthe.

L'application actuelle la plus importante de la théorie de la complexité est la cryptographie, qui est utilisée pour sécuriser des informations sur Internet, telles que les numéros de carte de crédit et les mots de passe. Les créateurs de cryptosystèmes, par exemple, doivent s'assurer que le décodage de leur système soit un problème NP, c'est-à-dire un problème que les ordinateurs mettraient des millions d'années à résoudre. Au début de sa carrière, A. Wigderson a apporté des contributions fondamentales à un nouveau concept en cryptographie : la preuve à divulgation nulle qui, plus de 30 ans plus tard, est aujourd'hui utilisée dans la technologie blockchain. Dans une preuve à divulgation nulle, deux personnes doivent prouver une affirmation sans révéler d'autre information que la validité de cette affirmation, comme l'exemple des deux millionnaires qui veulent prouver qui est plus riche sans qu'aucun des deux n'évoquent l'ampleur exacte de leur fortune. A. Wigderson, en collaboration avec Oded Goldreich et Silvio Micali, a démontré que les preuves à divulgation nulle peuvent être utilisées pour prouver, en secret, tout résultat public au sujet de données confidentielles. Imaginons, par exemple, que vous vouliez prouver à quelqu'un que vous avez démontré un théorème mathématique, mais sans révéler de détails sur votre façon de procéder. Vous pourrez le faire avec une preuve à divulgation nulle.

En 1994, A. Wigderson a remporté le prix Rolf Nevanlinna, décerné par l'Union mathématique internationale tous les quatre ans pour récompenser l'aspect informatique des mathématiques. Parmi ses nombreux autres prix figurent le Prix Gödel 2009 et le Prix Knuth 2019.

A. Wigderson est marié à Edna, qu'il a rencontré au Technion, et qui travaille au service informatique de l'Institute for Advanced Study. Ils ont trois enfants et deux petits-enfants.

Source de la citation : Portraits de Heidelberg Laureate Forum, entretien avec Avi Wigderson, 2017.