Lovász and Wigderson Awarded 2021 Abel Prize

The Norwegian Academy of Science and Letters has awarded the Abel Prize for 2021 to **László Lovász** of Eötvös Loránd University and **Avi Wigderson** of the Institute for Advanced Study "for their foundational contributions to theoretical computer science and discrete mathematics, and their leading role in shaping them into central fields of modern mathematics."

László Lovász

Avi Wigderson

Citation

Theoretical computer science (TCS) is the study of the power and limitations of computing. Its roots go back to the foundational works of Kurt Gödel, Alonzo Church, Alan Turing, and John von Neumann, leading to the development of real physical computers. TCS contains two complementary subdisciplines: algorithm design, which develops efficient methods for a multitude of computational problems, and computational complexity, which shows inherent limitations on the efficiency of algorithms. The notion of polynomial-time algorithms put forward in the 1960s by Alan Cobham, Jack Edmonds, and others and the famous $P \neq NP$ conjecture of Stephen Cook, Leonid Levin, and Richard Karp had strong impact on the field and on the work of Lovász and Wigderson.

Apart from its tremendous impact on broader computer science and practice, TCS provides the foundations of cryptography and is now having growing influence on several other sciences, leading to new insights therein by "employing a computational lens." Discrete structures such as graphs, strings, permutations are central to TCS, and naturally discrete mathematics and TCS have been closely allied fields. While both these fields have benefited immensely from more traditional areas of mathematics, there has been growing influence in the reverse direction as well. Applications, concepts, and techniques from TCS have motivated new challenges, opened new directions of research, and solved important open problems in pure and applied mathematics.

László Lovász and Avi Wigderson have been leading forces in these developments over the last decades. Their work interlaces in many ways, and, in particular, they have both made fundamental contributions to understanding randomness in computation and in exploring the boundaries of efficient computation.

Along with Arjen Lenstra and Hendrik Lenstra, László Lovász developed the LLL lattice reduction algorithm. Given a high-dimensional integer lattice (grid), this algorithm finds a nice, nearly orthogonal basis for it. In addition to several applications, such as an algorithm to factorize rational polynomials, the LLL algorithm is a favorite tool of cryptanalysts, successfully breaking several proposed cryptosystems. Surprisingly, the analysis of the LLL algorithm is also used to design and guarantee the security of newer, lattice-based cryptosystems that seem to withstand attacks even by quantum computers. For some exotic cryptographic primitives, such as homomorphic encryption, the only constructions known are via these lattice-based cryptosystems.

The LLL algorithm is only one among many of Lovász's visionary contributions. He proved the Local Lemma, a unique tool to show existence of combinatorial objects whose existence is rare, as opposed to the standard probabilistic method used when objects exist in abundance.

Along with Martin Grötschel and Lex Schrijver, he showed how to efficiently solve semidefinite programs, leading to a revolution in algorithm design. He contributed to the theory of random walks with applications to Euclidean isoperimetric problems and approximate volume computations of high-dimensional bodies. His paper with Uriel Feige, Shafi Goldwasser, Shmuel Safra, and Mario Szegedy on probabilistically checkable proofs gave an early version of the PCP Theorem, an immensely influential result showing that the correctness of mathematical proofs can be verified probabilistically, with high confidence, by reading only a small number of symbols! In addition, he also solved long-standing problems such as the perfect graph conjecture, the Kneser conjecture, determining the Shannon capacity of the pentagon graph, and, in recent years, developed the theory of graph limits (in joint work with Christian Borgs, Jennifer Chayes, Lex Schrijver, Vera Sós, Balázs Szegedy, and Katalin Vesztergombi). This work ties together elements of extremal graph theory, probability theory, and statistical physics.

Avi Wigderson has made broad and profound contributions to all aspects of computational complexity, especially the role of randomness in computation. A randomized algorithm is one that flips coins to compute a solution that is correct with high probability. Over decades, researchers discovered deterministic algorithms for many problems for which only a randomized algorithm was known before. The deterministic algorithm for primality testing, by Agrawal, Kayal, and Saxena, is a striking example of such a derandomized algorithm. These derandomization results raise the question of whether randomness is ever really essential. In works with László Babai, Lance Fortnow, Noam Nisan, and Russell Impagliazzo, Wigderson demonstrated that the answer is likely to be in the negative. Formally, they showed a computational conjecture, similar in spirit to the $P \neq NP$ conjecture, implies that $P = BPP$. This means that every randomized algorithm can be derandomized and turned into a deterministic one with comparable efficiency; moreover, the derandomization is generic and universal, without depending on the internal details of the randomized algorithm.

Another way to look at this work is as a tradeoff between hardness versus randomness: if there exists a hard enough problem, then randomness can be simulated by efficient deterministic algorithms. Wigderson's subsequent work with Impagliazzo and Valentine Kabanets proves a converse: efficient deterministic algorithms even for specific problems with known randomized algorithms would imply that there must exist such a hard problem. This work is intimately tied with constructions of pseudorandom (random looking) objects. Wigderson's works have constructed pseudorandom generators that turn a few truly random bits into many pseudorandom bits, extractors that extract nearly perfect random bits from an imperfect source of randomness, Ramsey graphs and expander graphs that are sparse and still have high connectivity. With Omer Reingold and Salil Vadhan, he introduced the zig-zag graph product, giving an elementary method to build expander graphs, and inspiring the combinatorial proof of the PCP Theorem by Irit Dinur and a memory efficient algorithm for the graph connectivity problem by Reingold. The latter gives a method to navigate through a large maze while remembering the identity of only a constant number of intersection points in the maze!

Wigderson's other contributions include zero-knowledge proofs that provide proofs for claims without revealing any extra information besides the claims' validity, and lower bounds on the efficiency of communication protocols, circuits, and formal proof systems.

Thanks to the leadership of Lovász and Wigderson, discrete mathematics and the relatively young field of theoretical computer science are now established as central areas of modern mathematics.

Biographical Sketch: László Lovász

Note: This biographical information is taken from the Abel Prize website: `https://www.abelprize.no/c76389/binfil/download.php?tid=76360`

A mathematical star since he was a teenager, László Lovász has more than delivered on his early promise, becoming one of the most prominent mathematicians of the last half century. His work has established connections between discrete mathematics and computer science, helping to provide theoretical foundations, as well as design practical applications, for these two large and increasingly important areas of scientific study. He has also served his community as a prolific writer of books, noted for their clarity and accessibility, as an inspirational lecturer, and as a leader, spending a term as president of the International Mathematical Union (2007–2010).

Born in 1948 in Budapest, Lovász was part of a golden generation of young Hungarian mathematicians, nurtured by the country's unique school mathematics culture. He was in the first group of an experiment in which gifted students at a Budapest high school were given specialist math classes. (One of his classmates was Katalin Vesztergombi, whom he later married.) Lovász excelled, winning gold medals in the 1964, 1965, and 1966 International Mathematics Olympiads, on the latter two occasions with perfect scores. He also won a primetime Hungarian TV show in which students were placed in glass cages and asked to solve math problems.

Perhaps the most important encounter in his teenage years, however, was with his mathematical hero, Paul Erdős, the nomadic and famously sociable Hungarian mathematician. Erdős was an insatiable sharer of problems and inspired Lovász to work in "Hungarian-style combinatorics," essentially concerned with properties of graphs.

Not only did this set up an initial research direction, but it also paved the way for Lovász's style of how to do math: openly and collaboratively.

Lovász attended Eötvös Loránd University in Budapest. He was awarded a PhD (or rather, the Hungarian equivalent, the CSc) at age twenty-two in 1970, by which time he had already lectured at international conferences and had fifteen papers published. Due to a quirk of the Hungarian system, he only graduated in 1971, a year after he got his PhD.

Combinatorics is the math of patterns and counting patterns. Graph theory is the math of connections, such as in a network. Both come under the umbrella of "discrete" math, since the objects of study have distinct values, rather than varying smoothly like, say, a point moving along a curve. Erdős liked to study these areas for purely intellectual pleasure, with no concern for their usefulness in the real world. Lovász, on the other hand, became a leader of a new generation of mathematicians who realized that discrete math had, in computer science, a thrilling new area of application.

In the 1970s, for example, graph theory became one of the first areas of pure mathematics able to illuminate the new field of computational complexity. Indeed, one of the major impacts of Lovász's work has been to establish ways in which discrete math can address fundamental theoretical questions in computer science.

Among his contributions to the foundational underpinning of computer science are powerful algorithms with wide-ranging applications. One of these, the LLL algorithm, named after Lovász and the brothers Arjen and Hendrik Lenstra, represented a conceptual breakthrough in the understanding of lattices, a basic geometrical object, and which has had remarkable applications in areas including number theory, cryptography, and mobile computing. Currently, the only known encryption systems that can withstand an attack by a quantum computer are based on lattices and use the LLL algorithm.

During the 1970s and 1980s, Lovász was based in Hungary, first at Eötvös Loránd University and then at József Attila University in Szeged, where he became chair of Geometry in 1978. He returned to Eötvös Loránd in 1982 to be chair of Computer Science. In those early decades he solved important and far-reaching problems in many areas of discrete mathematics. One of his first major results, in 1972, was to resolve the "perfect graph conjecture," a long-standing open problem in graph theory. In 1978 he settled Kneser's conjecture, again in graph theory, but this time surprising his colleagues by using a proof from algebraic topology, a completely different area. In 1979 he solved a classical problem in information theory, determining the "Shannon capacity" of the pentagon graph.

A major theme of Lovász's work in both combinatorics and algorithm design is the investigation of probabilistic methods. The discovery in this area for which he is best known is the Lovász Local Lemma, an important and frequently used tool in probabilistic combinatorics used to establish the existence of rare objects, as opposed to the more standard tools used when objects are more abundant. Lovász also contributed to an early, influential paper on probabilistically checkable proofs (PCP), which grew into one of the most important areas of computational complexity.

In 1993, Lovász was appointed William K. Lanman Professor of Computer Science and Mathematics at Yale University. In 1999, he left academia to take up a position as a Senior Researcher at Microsoft, before returning in 2006 to Eötvös Loránd University, where he is currently a professor.

Lovász has traveled widely. He has held visiting positions at the universities of Vanderbilt in Nashville, Tennessee (1972–1973), Waterloo (1978–1979), Bonn (1984–1985), Chicago (1985), Cornell (1985), and Princeton (1989–1993), as well as spending a year at the Institute for Advanced Study in Princeton (2011–2012). Called "Laci" by friends and colleagues, he is known for his modesty, generosity, and openness. These qualities have led to positions on the executive committee of the International Mathematical Union (including as president), and at the Hungarian Academy of Sciences (where he was president from 2014 to 2020).

Lovász has won many awards, including the 1999 Wolf Prize, the 1999 Knuth Prize, the 2001 Gödel Prize, and the 2010 Kyoto Prize.

He has four children with Katalin Vesztergombi, a mathematician who is also one of his frequent collaborators, and seven grandchildren.

Biographical Sketch: Avi Wigderson

Note: This biographical information is taken from the Abel Prize website: `https://www.abelprize.no/c76389/binfil/download.php?tid=76359`

When Avi Wigderson began his academic career in the late 1970s, the theory of "computational complexity"—which concerns itself with the speed and efficiency of algorithms—was in its infancy. Wigderson's contribution to enlarging and deepening the field is arguably greater than that of any single other person, and what was a young subject is now an established field of both mathematics and theoretical computer science. Computational complexity has also become unexpectedly important, providing the theoretical basis for Internet security.

Wigderson was born in Haifa, Israel, in 1956. He entered Technion, the Israeli Institute of Technology, in 1977, and graduated with a BSc in computer science in 1980. He moved to Princeton for his graduate studies, receiving his PhD in 1983 for the thesis *Studies in Combinatorial Complexity*, for which Richard Lipton was his advisor. In 1986,

Wigderson returned to Israel to take up a position at the Hebrew University in Jerusalem. He was given tenure the following year and made full professor in 1991.

In the 1970s, computer theoreticians framed certain fundamental ideas about the nature of computation, notably the notions of P and NP. P is the set of problems that computers can solve easily, say, in a few seconds, whereas NP also contains problems that computers find hard to solve, meaning that the known methods can only find the answer in, say, millions of years. The question of whether all these hard problems can be reduced to easy ones, that is, whether or not P = NP, is the foundational question of computational complexity. Indeed, it is now considered one of the most important unsolved questions in all of mathematics.

Wigderson made stunning advances in this area by investigating the role of randomness in aiding computation. Some hard problems can be made easy using algorithms in which the computer flips coins during the computation. If an algorithm relies on coin flipping, however, there is always a chance that an error can creep into the solution. Wigderson, first together with Noam Nisan and later with Russell Impagliazzo, showed that for any fast algorithm that can solve a hard problem using coin flipping, there exists an almost-as-fast algorithm that does not use coin flipping, provided certain conditions are met.

Wigderson has conducted research into every major open problem in complexity theory. In many ways, the field has grown around him, not only because of his breadth of interests, but also because of his approachable personality and enthusiasm for collaborations. He has coauthored papers with well over 100 people and has mentored a large number of young complexity theorists.

In 1999, Wigderson joined the Institute for Advanced Study (IAS) in Princeton, where he has been ever since. At an event to celebrate Wigderson's sixtieth birthday in 2016, IAS director Robbert Dijkgraaf said that he had launched a golden age of theoretical computer science at the institute.

Wigderson is known for his ability to see links between apparently unrelated areas. He has deepened the connections between mathematics and computer science. One example is the "zig-zag graph product," which he developed with Omer Reingold and Salil Vadhan, which links group theory, graph theory, and complexity theory and has surprising applications, such as how best to get out of a maze.

The most important present-day application of complexity theory is to cryptography, which is used to secure information on the Internet, such as credit card numbers and passwords. People who design cryptosystems, for example, must make sure that the task of decoding their system is an NP problem, that is, one that would take computers millions of years to achieve. Early in his career, Wigderson made fundamental contributions to a new concept in cryptography, the zero-knowledge proof, which more than thirty years later is now being used in blockchain technology. In a zero-knowledge proof, two people must prove a claim without revealing any knowledge beyond the validity of that claim, such as the example of the two millionaires who want to prove who is richer without either of them letting on how much money they have. Wigderson, together with Oded Goldreich and Silvio Micali, showed that zero-knowledge proofs can be used to prove, in secret, any public result about secret data. Just say, for example, that you want to prove to someone that you have proved a mathematical theorem, but you don't want to reveal any details of how you did it, a zero-knowledge proof will allow you to do this.

In 1994, Wigderson won the Rolf Nevanlinna Prize for computer science, which is awarded by the International Mathematical Union every four years. Among his many other prizes are the 2009 Gödel Prize and the 2019 Knuth Prize.

Wigderson is married to Edna, whom he met at the Technion, and who works in the computer department of the Institute for Advanced Study. They have three children and two grandchildren.

About the Prize

The Niels Henrik Abel Memorial Fund was established in 2002 to award the Abel Prize for outstanding scientific work in the field of mathematics. It carries a cash award of 7.5 million Norwegian krone (approximately US$720,000). The prize is awarded by the Norwegian Academy of Science and Letters, and the choice of Abel Laureate is based on the recommendation of the Abel Committee, which consists of five internationally recognized research scientists in the field of mathematics. The Committee is appointed for a period of two years.

Read more about the recipients' life and work, as well as a list of previous recipients of the Abel Prize, at `https://www.abelprize.no/c76018/seksjon/vis.html?tid=76019&strukt_tid=76018`.

—From announcements of the Norwegian Academy of Science and Letters

Credits

Photo of László Lovász is courtesy of László Mudra/Hungarian Academy of Sciences.

Photo of Avi Wigderson is courtesy of Dan Komoda, Institute for Advanced Study.