

Laszlo Lovasz and Avi Wigderson share the 2021 Abel Prize

by Abhigyan Ray - Saturday, March 20, 2021

<https://gonitsora.com/laszlo-lovasz-and-avi-wigderson-share-2021-abel-prize/>

Last time the phrase "theoretical computer science" found mention in an Abel Prize citation was in 2012 when the legendary Hungarian mathematician, Endre Szemerédi was awarded mathematics' highest honour. During the ceremony, László Lovász and Avi Wigderson were there to offer a primer into the majestic contributions of the laureate. Little did they know, nearly a decade later, they both would be joint recipients of the award. The Norwegian Academy of Science and Letters has awarded the 2021 Abel Prize to László Lovász of Eötvös Loránd University in Budapest, Hungary and Avi Wigderson of the Institute for Advanced Study, Princeton, USA, "for their foundational contributions to theoretical computer science and discrete mathematics, and their leading role in shaping them into central fields of modern mathematics." Widely hailed as the mathematical equivalent of the Nobel Prize, this year's Abel goes to two trailblazers for their revolutionary contributions to the mathematical foundations of computing and information systems. The citation of the award can be found [here](#).

László Lovász

Lovász bagged three gold medals at the International Mathematical Olympiad, from 1964 to 1966, and received his Candidate of Sciences (Ph.D. equivalent) degree in 1970 at the Hungarian Academy of Sciences advised by Tibor Gallai. Lovász was initially based in Hungary, at Eötvös Loránd University and József Attila University, and in 1993 he was appointed William K Lanman Professor of Computer Science and Mathematics at Yale University. In 1999, he had a brief sojourn as a Senior Researcher at Microsoft, before returning in 2006 to Eötvös Loránd University, where he is currently a professor. A product of the legendary Budapest School of Mathematics, László represents the long line of distinguished Hungarian mathematicians right from János Bolyai and the Riesz brothers, Frigyes and Marcel; to Gábor Szegő; Alfréd Rényi; John von Neumann; Paul Turán; [Paul Erdős](#); Raoul Bott, Peter Lax, [Endre Szemerédi](#). Early encounters with Erdős influenced Lovász to work in 'Hungarian-style combinatorics', essentially concerned with properties of graphs.

In 1972, Lovász proved the weak perfect graph conjecture, utilising the paradigm of expressing discrete structures by systems of linear inequalities. In 1979, he solved a famous and long-standing open problem on Shannon capacity of the pentagon in the field of information theory, introducing quadratic forms to express discrete structures and heralding in the era of semidefinite programming, a central topic in mathematical optimization and revolutionising algorithm design. He also resolved Kneser's conjecture, borrowing tools from algebraic topology, and played a pioneering role in the development of the geometric methodology of algorithms based on the ellipsoid method, which led to the solution of a major open problem on submodular function minimization. Through the Lovász local lemma, he provided a fundamental tool of probabilistic methods for the analysis of discrete structures and contributed to the PCP characterization of NP and its connection to the hardness of approximation while simultaneously constructing important algorithms like the matroid matching algorithm and the basis reduction algorithm for integer lattices (LLL). The reduction algorithm, commonly known as the LLL (Lenstra–Lenstra–Lovász lattice basis reduction algorithm named after Lovász and the brothers Arjen and

Hendrik Lenstra) algorithm, is one of the basic tools of cryptography and is a fundamental algorithm for solving lattice problems. It was famously used by Andrew Odlyzko and Herman te Riele in disproving the Mertens conjecture. Decades later, LLL still has numerous applications in number theory, integer programming, and cryptography.

Avi Wigderson

Wigderson completed his undergraduate studies at the Technion in Israel and went on to receive a Ph.D. in computer science at Princeton under the supervision of Richard Lipton in 1983. He then served as a Visiting Assistant Professor at UC Berkeley, a Visiting Scientist at IBM, and a Fellow at MSRI in Berkeley before joining the Hebrew University as a faculty member in 1986, and since 1999, Wigderson has been the Herbert H. Maass Professor in the School of Mathematics at the Institute for Advanced Study, Princeton. Wigderson has made profoundly fundamental contributions to the foundations of computing in areas like randomised computation, cryptography, and computational complexity.

In a landmark series of results, Wigderson proved under certain computational assumptions that every probabilistic polynomial time algorithm can be fully derandomized., i.e., randomness is not necessary for polynomial-time computation, providing strong evidence for $P = BPP$. In cryptography, Wigderson showed how one could compute any function securely in the presence of dishonest parties; showcased the existence of zero-knowledge proofs, proofs that yield nothing but their validity; and helped define the model of multiprover interactive proofs that eventually led to the celebrated PCP theorem. Wigderson also provided lower bounds on the efficiency of communication protocols, circuits, and formal proof systems. and gave the first efficient combinatorial constructions of expander graphs (the zig-zag graph product), an important class of highly connected sparse graphs, and subsequently inspired many important results.

Conclusion

Wigderson and Lovász have additionally, and very successfully, donned hats of terrific mentors, able administrators, wonderful expositors, and inspirational leaders. Their fantastic books and fascinating lectures have stimulated mathematical research around the world. Wigderson has trained many generations of theoretical computer scientists at the Institute for Advanced Study whilst for many, Lovász's Combinatorial Problems and Exercises is a necessary and serendipitous initiation to the world of combinatorics. Lovász was President of the International Mathematical Union from 2007 to 2010, and also headed the Hungarian Academy of Sciences from 2014 to 2020, strongly pushing back against the farcical policies of the far right government.

Wigderson and Lovász's phenomenal work has found significantly incredible real-world applications. Brin and Page relied on Lovász's spectral graph theory results to develop PageRank, the backbone of Google Search, whilst Wigderson's work on zero knowledge proofs underpins the technology behind blockchains and cryptocurrencies. Apart from applications to devising stronger cryptographic systems, their work catalyses advances in neuroscience, quantum physics, statistical mechanics, economics, social sciences, and medicine, displaying the ubiquity of fundamental basic science research in driving modern day technological advances. Wigderson and Lovász not only introduced visionary and powerful concepts but also solved formidable problems and their work is characterised by extraordinary depth, technical

power, creative synthesis of ideas and methods from vast swathes of mathematics and computer science. Through their monumental contributions, effortlessly transcending boundaries between pure and applied mathematics, the two giants of modern day science and mathematics have resoundingly demonstrated that theoretical computer science is fundamentally and intrinsically a part of mathematics.

Some words on Theoretical Computer Science and Discrete Mathematics

Theoretical Computer Science is the study of the power and limitations of computing. It contains two complementary sub-disciplines: 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?NP conjecture of Stephen Cook, Leonid Levin, and Richard Karp had a very strong impact on the field.

Discrete mathematics is the study of structures such as graphs, sequences, permutations, and geometric configurations. The combinatorics of discrete structures is also a major component of many areas of pure mathematics, including number theory, probability, algebra, geometry, and analysis. Combinatorics is the study of patterns and graph theory is the study of connections such as in a network. Both come under the umbrella of 'discrete' maths, since the objects of study have distinct values, rather than varying smoothly like a point moving along a curve. The mathematics of such structures forms the foundation of theoretical computer science and information theory. For instance, communication networks such as the internet can be described and analyzed using the tools of graph theory, and the design of efficient computational algorithms relies crucially on insights from discrete mathematics.

PDF generated from <https://gonitsora.com/laszlo-lovasz-and-avi-wigderson-share-2021-abel-prize/>.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.