THE ABEL PRIZE 2021

The Norwegian Academy of Science and Letters has decided to award the Abel Prize for 2021 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."

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 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 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 crypto-systems. Surprisingly, the analysis of the LLL algorithm is also used to design and guarantee the security of newer, lattice-based crypto-systems 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 crypto-systems.

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≠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 trade-off 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.