Citation: 2012 Knuth Prize

The 2012 Knuth Prize has been awarded to Leonid Levin, in recognition of four decades of visionary research in complexity, cryptography, and information theory.

Professor Levin is best known for his discovery of NP-completeness, the core concept of computational complexity and the best explanation to date of why one expects certain computational problems to be intractable. He made this discovery in the Soviet Union at about the same time as, but independently of, Stephen Cook, the winner of the 1982 Turing Award. His work on the subject did not appear in the West until 1973, by which time the study of NP-completeness was well established, following Cook's 1971 STOC paper; for a long time, Levin received little official recognition for his conceptual breakthrough. Fortunately, it is now common for computational-complexity textbooks to refer to the "Cook-Levin Theorem." Later, Levin developed the theory of "average-case NP-completeness," which has given us the best explanation to date of why some computational problems are intractable not only on rare, contrived instances but "on average," with respect to input distributions of interest. He also provided a key step, with co-authors László Babai, Lance Fortnow, and Mario Szegedy, in the proof of the celebrated PCP Theorem that relates the complexity of solving certain natural NP-hard search problems approximately to the complexity of solving them exactly. Together, they put forth the notion of "holographic proofs," *i.e.*, proofs whose correctness can be checked efficiently by a program that samples only a small fraction of the bits.

In cryptographic theory, Levin is well known, with co-author Oded Goldreich, for the "Goldreich-Levin hardcore bit." He and Goldreich discovered a general method for transforming any one-way function into a predicate whose value cannot be predicted efficiently with probability significantly greater than ½. Their construction is an essential ingredient in many subsequent key results. Together with Johan Håstad, Russell Impagliazzo, and Michael Luby, Levin showed that the existence of computationally secure pseudorandom-number generators is equivalent to the existence of one-way functions; the ingenious "HILL construction" resolved a long-standing open problem in cryptography.

In Kolmogorov complexity, Levin changed the landscape by discovering (at the same time as, but independently of, Kolmogorov) the approximate symmetry of "algorithmic information." He developed the universal measure and adjustments of Kolmogorov complexity that enable us to characterize the randomness of infinite sequences. Currently, his uniform-randomness tests and information-conservation results are essential tools in the research area of algorithmic information.

Leonid Anatolievich Levin was born in 1948 in Dnipropetrovsk, Ukraine. He obtained a Masters degree in 1970 and a Ph.D. equivalent in 1972 at Moscow University, where he studied under Andrey Kolmogorov. He emigrated to the US in 1978 and earned a Ph.D. at MIT in 1979, where his advisor was Albert Meyer. Since 1980, he has been at Boston University, where he is currently a Professor in the Computer Science Department. He lives in Newton, MA, with his wife Larissa, a biologist and former faculty member at the University of Massachusetts Medical School; they have three children and two grandchildren.