2019 Knuth prize is Awarded to Avi Wigderson

March 23, 2019

The 2019 Donald E. Knuth Prize will be awarded to Avi Wigderson of the Institute for Advanced Study for fundamental and lasting contributions to the foundations of computer science in areas including randomized computation, cryptography, circuit complexity, proof complexity, parallel computation, and our understanding of fundamental graph properties. Wigderson has also trained many generations of theoretical computer scientists through his visitor and postdoc program at the Institute for Advanced Study.

Wigderson's work revolutionized our understanding of randomness in computation. In a series of results, he showed under widely-believed computational assumptions that every probabilistic polynomial time algorithm can be fully derandomized. In other words, randomness is not necessary for polynomial-time computation. This was achieved by a sequence of papers of his: "Hardness vs. Randomness" with Nisan, "BPP Has Subexponential Time Simulations Unless EXPTIME has Publishable Proofs" with Babai, Fortnow and Nisan, and "P=BPP if E Requires Exponential Circuits: Derandomizing the XOR Lemma" with Impagliazzo. This last result showed that P=BPP is implied by the assumption that there exist functions that can be computed by exponential-time Turing machines that cannot be computed by subexponential-size circuits in the worst case. To this day, the Impagliazzo-Wigderson paper is one of the strongest pieces of evidence we have that P = BPP.

In cryptography, in two landmark papers, one with Goldreich and Micali and one with Ben-Or and Goldwasser, Wigderson showed how one could compute any function securely in the presence of dishonest parties. Wigderson also with Goldreich and Micali showed that all problems with short proofs (i.e., all problems in NP) in fact have *zero-knowledge* proofs: that is, proofs that yield nothing but their validity, a central cryptographic construct.

Additionally, originating from cryptography but with applications to many areas in theoretical computer science, Wigderson with Ben-Or, Gold-

wasser, and Kilian defined the model of multiprover interactive proofs. This model for the first time showed how it would be possible for a polynomial-time machine to verify an exponentially-long proof. This idea had substantial impact, and among other things it led to the celebrated PCP theorem and the flow of follow-up works on hardness of approximation.

In the area of parallel computation, Wigderson provided a series of foundational results about parallel computing models. This includes the first RNC algorithm for constructing a perfect matching in a graph with Karp and Upfal, the first NC algorithm for finding a maximal independent set in a graph with Karp, and a number of fundamental lower bound results.

With Reingold, Vadhan and Capalbo, Wigderson gave the first efficient combinatorial constructions of expander graphs, an important class of highly connected sparse graphs. Before this work, only algebraic constructions had been known. Widgerson's development of combinatorial expander constructions enabled a series of important subsequent results including Reingold's deterministic logspace algorithm for st-connectivity.

In addition to specific research results, during his academic career Wigderson has supervised a large number of postdocs and PhD students. He also has written many expository and survey articles, such as the award winning survey "Expander Graphs and their Applications", and he recently published the book "Mathematics and Computation".

Wigderson received his PhD from Princeton University 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. Since 1999, Wigderson has been a Professor in the School of Mathematics at the Institute for Advanced Study.

Prize Committee: Avrim Blum, Chair (TTIC), Alan Frieze (CMU), Shafi Goldwasser (UC Berkeley), Noam Nisan (Hebrew U.), Ronitt Rubinfeld (MIT and Tel Aviv U.), and Andy Yao (Tsinghua U.).